NSIPS Security Overview

This is an automated presentation, but the arrow keys on your keypad can be used to navigate through the presentation.

If you would like to speed up the presentation press the down arrow key.

If the action has moved to fast and you need to repeat the action press the up arrow key and then the right arrow key.

Click to advance

Client to Web Transition

- To access NSIPS Web from a NMCI computer:
  - Type ‘Homeport’ in the Address box in Internet Explorer
  - Locate Personnel Forms and Records under the My SeaBag Section of the NMCI Home page. (Left side of the page)
  - Mouse over and select NSIPS from the Menu links that appear
- Or use https://nsips.nmci.navy.mil/ as a direct link
- With proper PKI certs and CAC card readers this link can be used for legacy systems

Click to advance

Client to Web Transition

- This presentation is designed to give an overview of the new security processes in NSIPS/ESR, to allow for an easy transition from Client Server(C-S)

- The topics covered will be
  - The SAAR Form
    - Individual User
    - Web Adhoc
    - Self Serve
  - ISSO/FAM/NAM Functions
  - Report Processes

Click to advance

Acronym Terminology

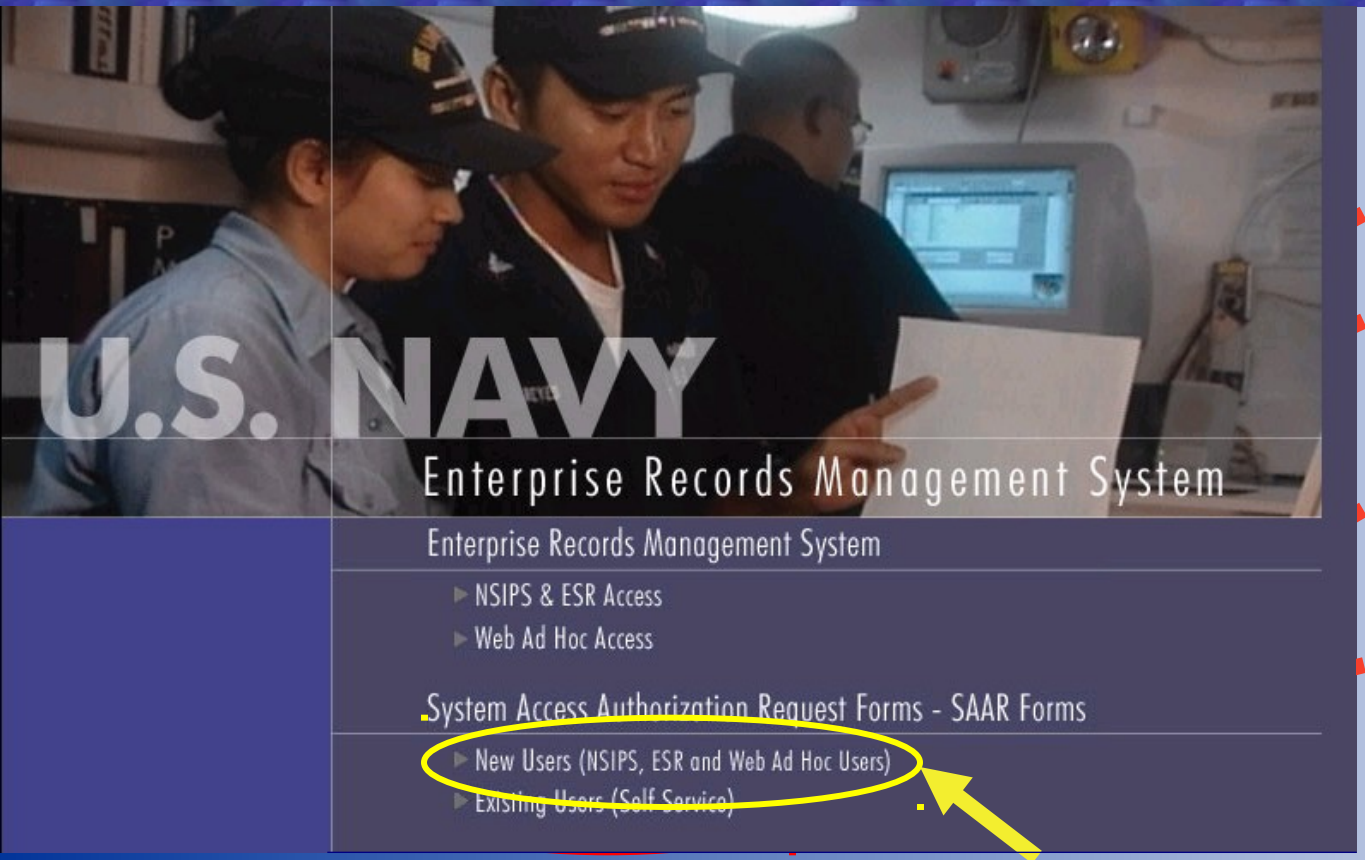
Definitions of Acronyms used in this presentation

- NSIPS - Navy Standard Integrated Personnel System
- NAM - NSIPS Access Manager
- ISSO - Information System Security Offi
- FAM - Functional Area Manager
- ESR - Electronic Service Record
- ERMS - Enterprise Record Management System
- PRA - Pay Record Accessibility
- UIC - Unit Identification Code
- PSA - Personnel Support Activity
- PSD - Personnel Support Detachment
- PLR - Pass Liaison Representative

In the NSIPS application the NAM, ISSO, and FAM are considered to be the same role.

Click to advance

Access to NSIPS/ESR


U.S. NAVY
Enterprise Records Management System
Enterprise Records Management System
NSIPS & ESR Access
Web Ad Hoc Access
System Access Authorization Request Forms - SAAR Forms
New Users (NSIPS, ESR and Web Ad Hoc Users)

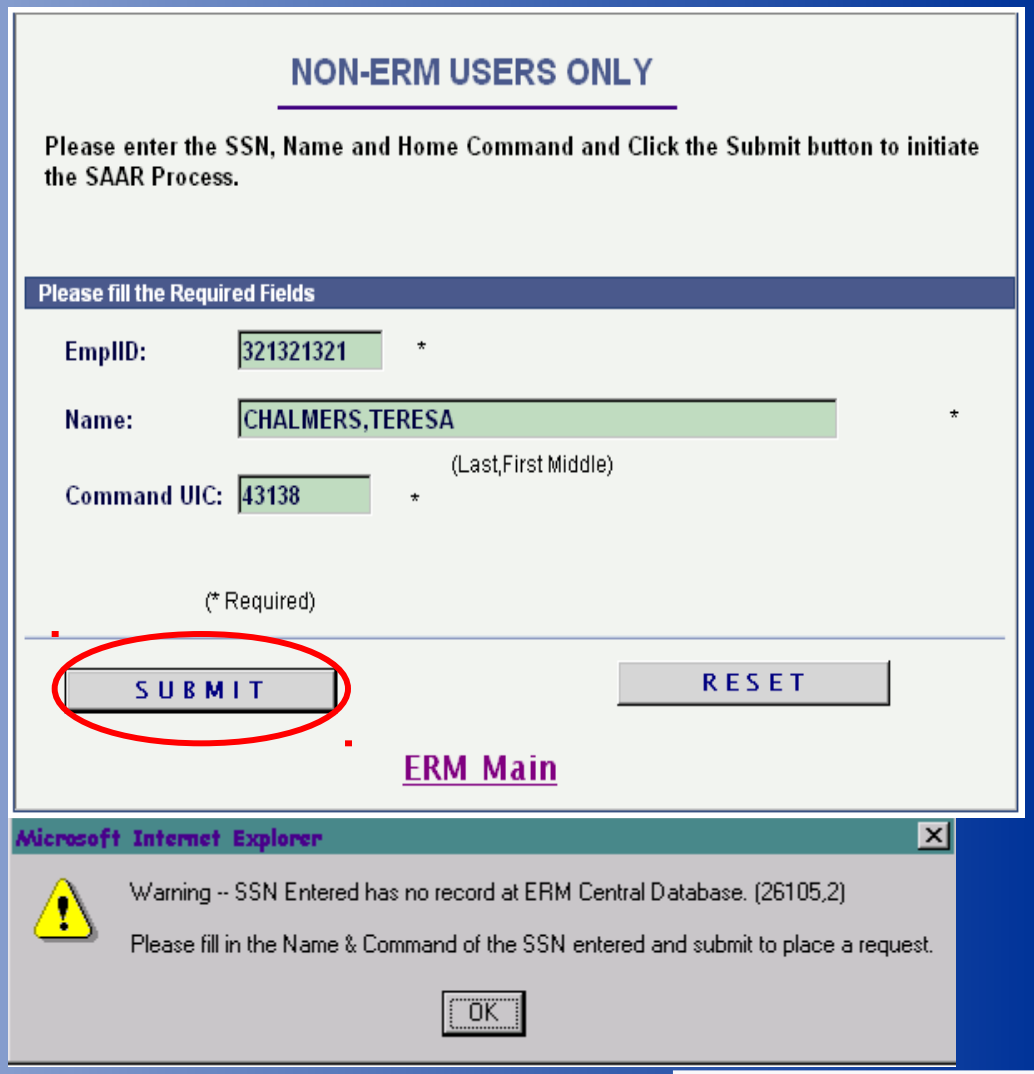
- From this screen, access the:
- Log-on screen
- Web Adhoc query system
- SAAR forms for New Users
- Self Service for existing Military members

- From this page the New Users link will be selected to open the SAAR form in order to create a new User account.

Click to advance

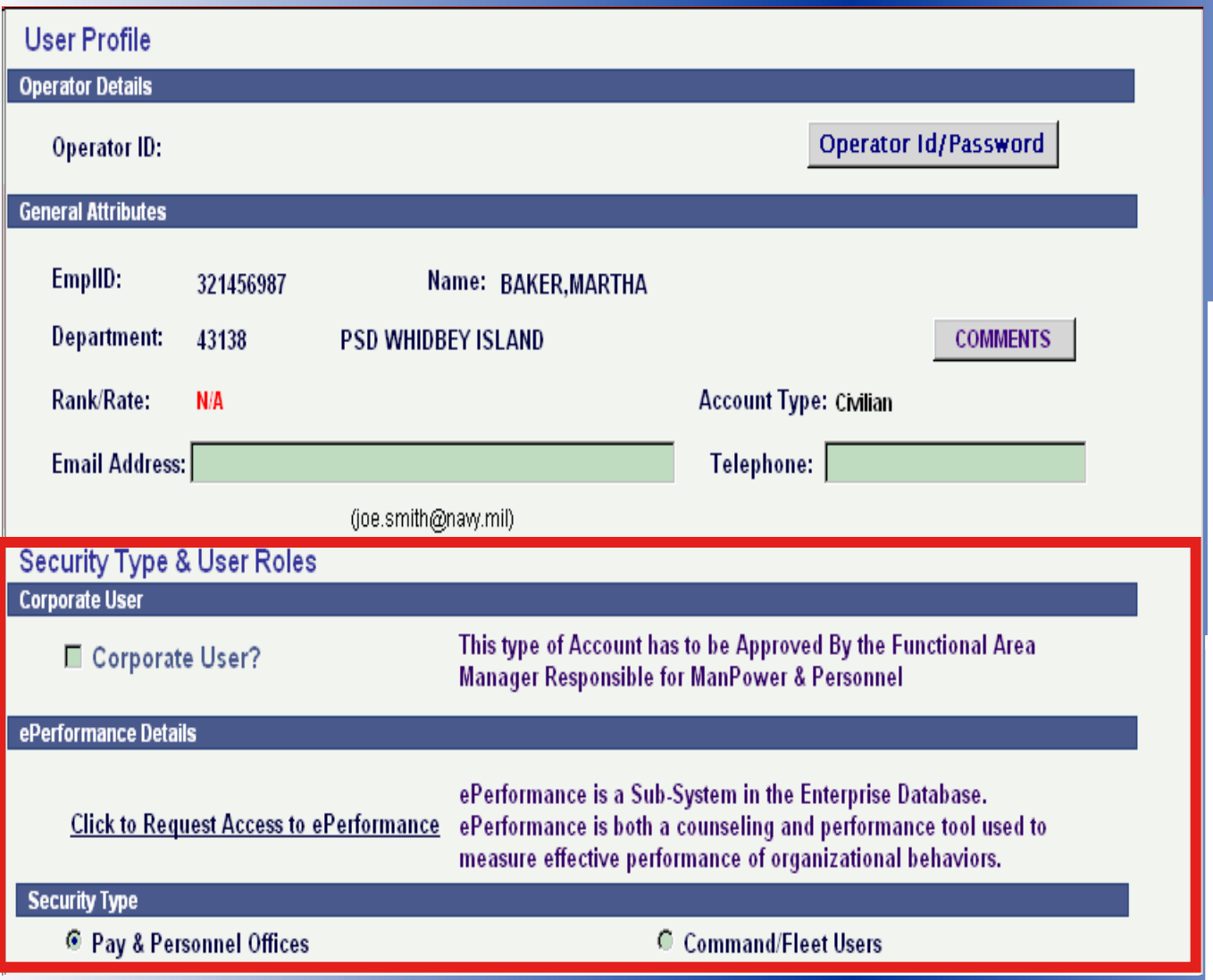
SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form

- ALL users will need to submit a SAAR in order to have access to NSIPS/ESR web
- Enter the SSN – If Military the name and UIC will prefill
- If the SSN does not exist, the user will be prompted to manually enter the name and UIC to create a civilian account
- The reset button will clear the above text fields
- Select the submit button to open the SAAR


NON-ERM USERS ONLY
Please enter the SSN, Name and Home Command and Click the Submit button to initiate the SAAR Process.
Please fill the Required Fields
EmplID: 321321321 *
Name: CHALMERS,TERESA *
(Last,First Middle)
Command UIC: 43138 *
(* Required)
SUBMIT
RESET
ERM Main
Microsoft Internet Explorer
Warning -- SSN Entered has no record at ERM Central Database. (26105,2)
Please fill in the Name & Command of the SSN entered and submit to place a request.
OK

Click to advance

SAAR Form, Sections



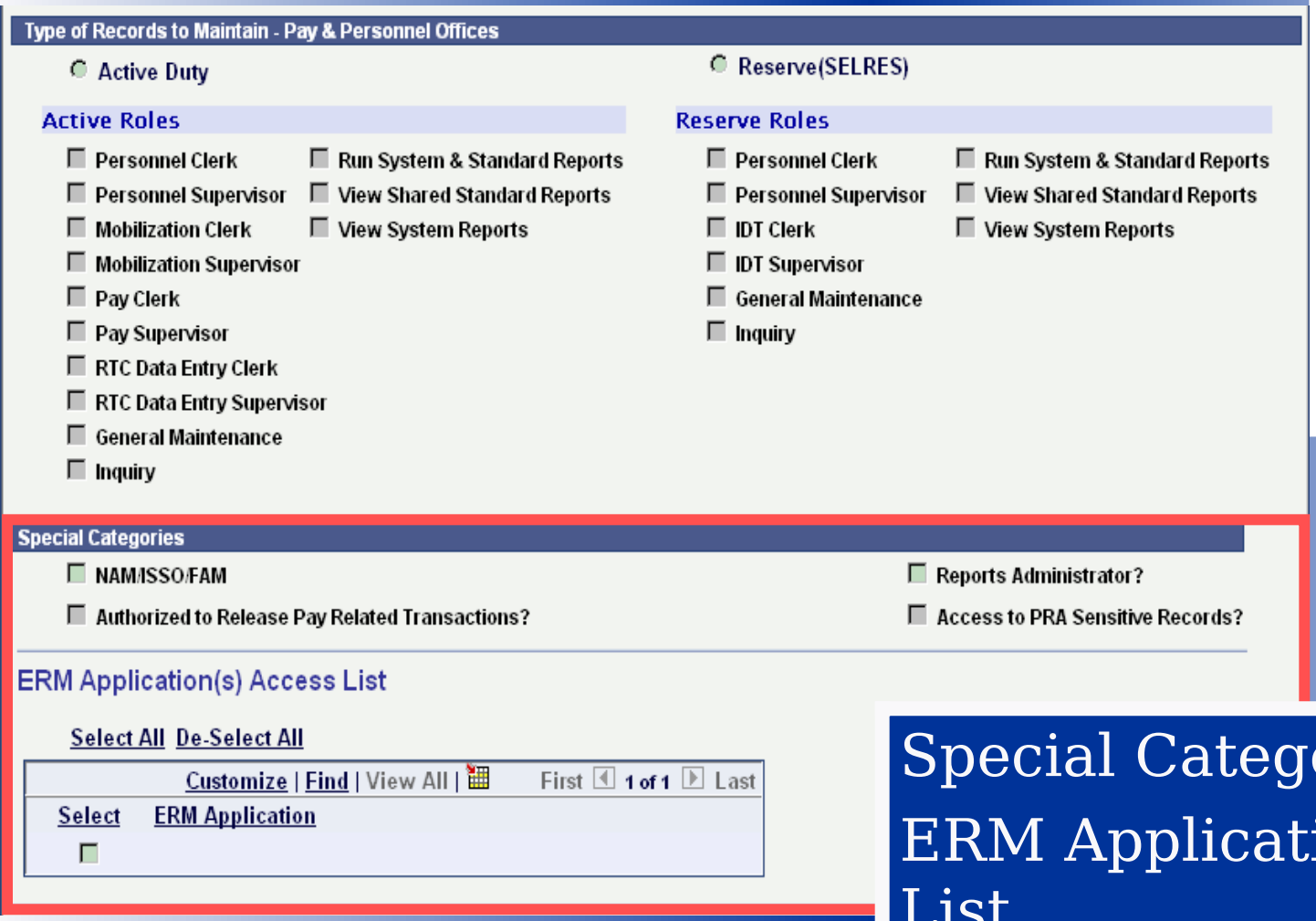
User Profile: Setting up an Operator Id and Password

General Attributes: Entering Email, Telephone

Corporate User account Type of records to be maintained:

Click to advance

SAAR Form Sections, cont.



Type of Records Maintained and Users Roles

Special Categories

ERM Applications Access List

Click to advance

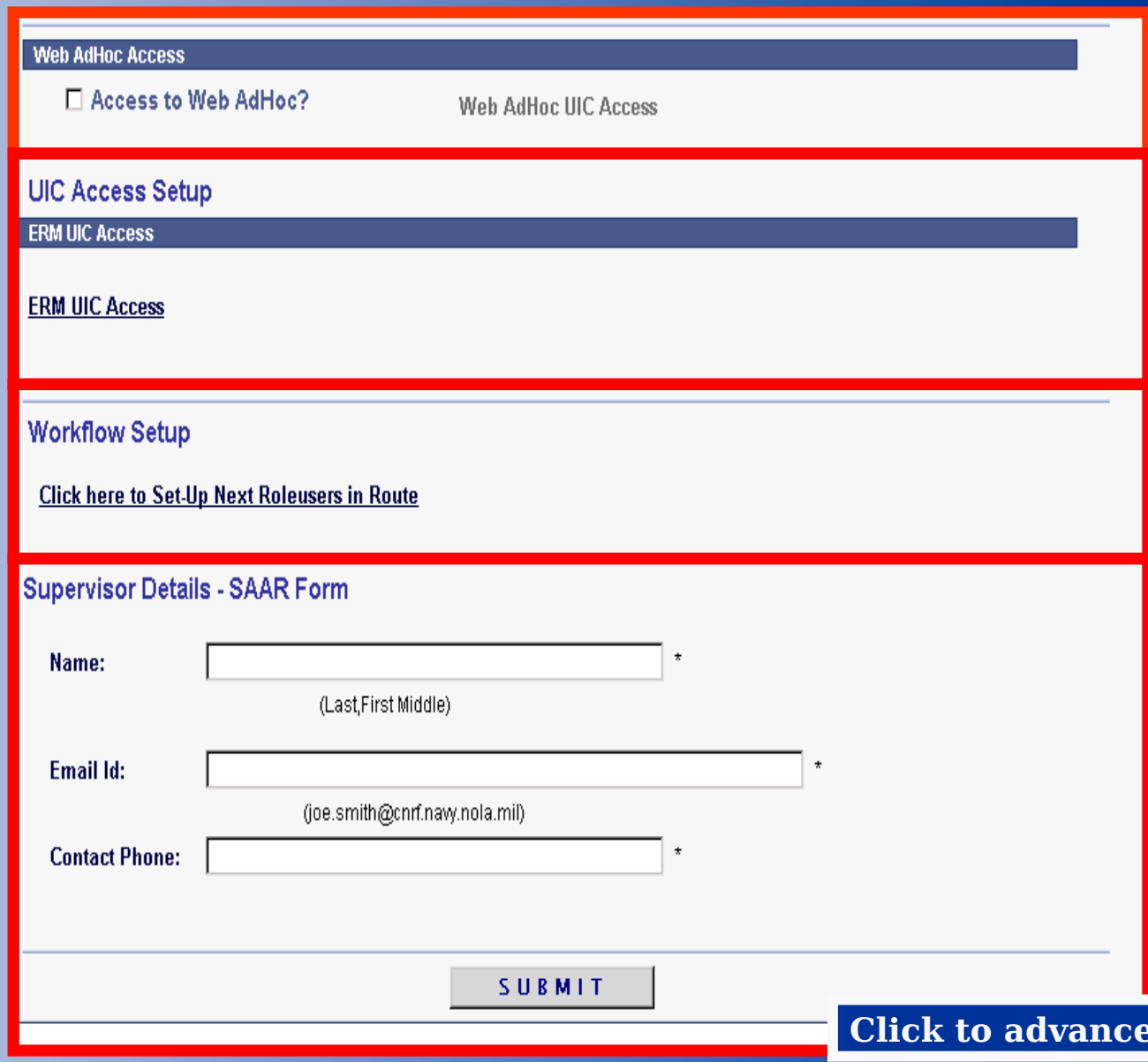
SAAR Form Sections, cont.

Web Adhoc Access

ERM UIC Access

Workflow Setup

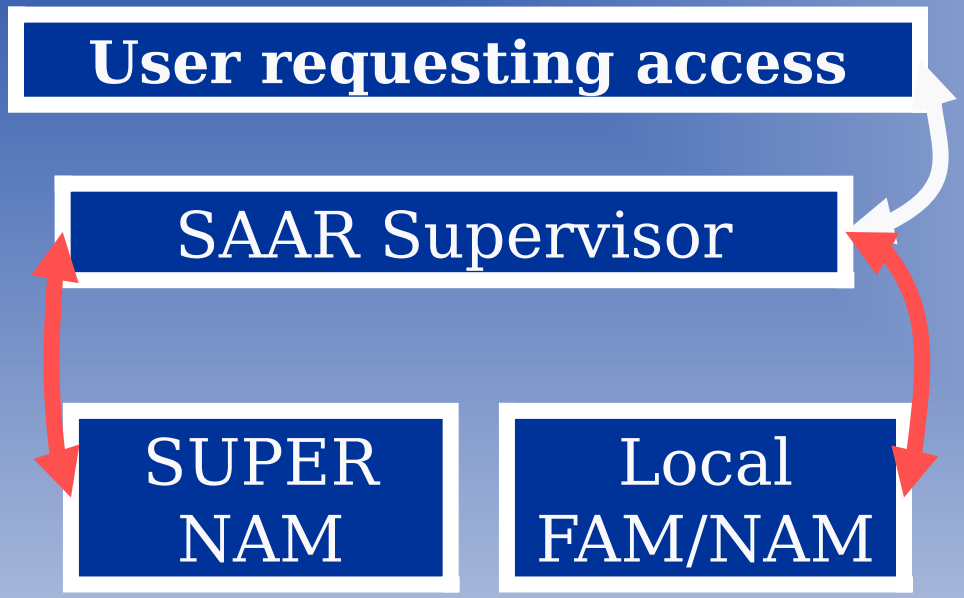
Supervisor Details



Click to advance

System Access Authorization Request (SAAR) Form, cont.

The routing of the SAAR request is as follows:



The SAAR Supervisor is the first step in the approval process

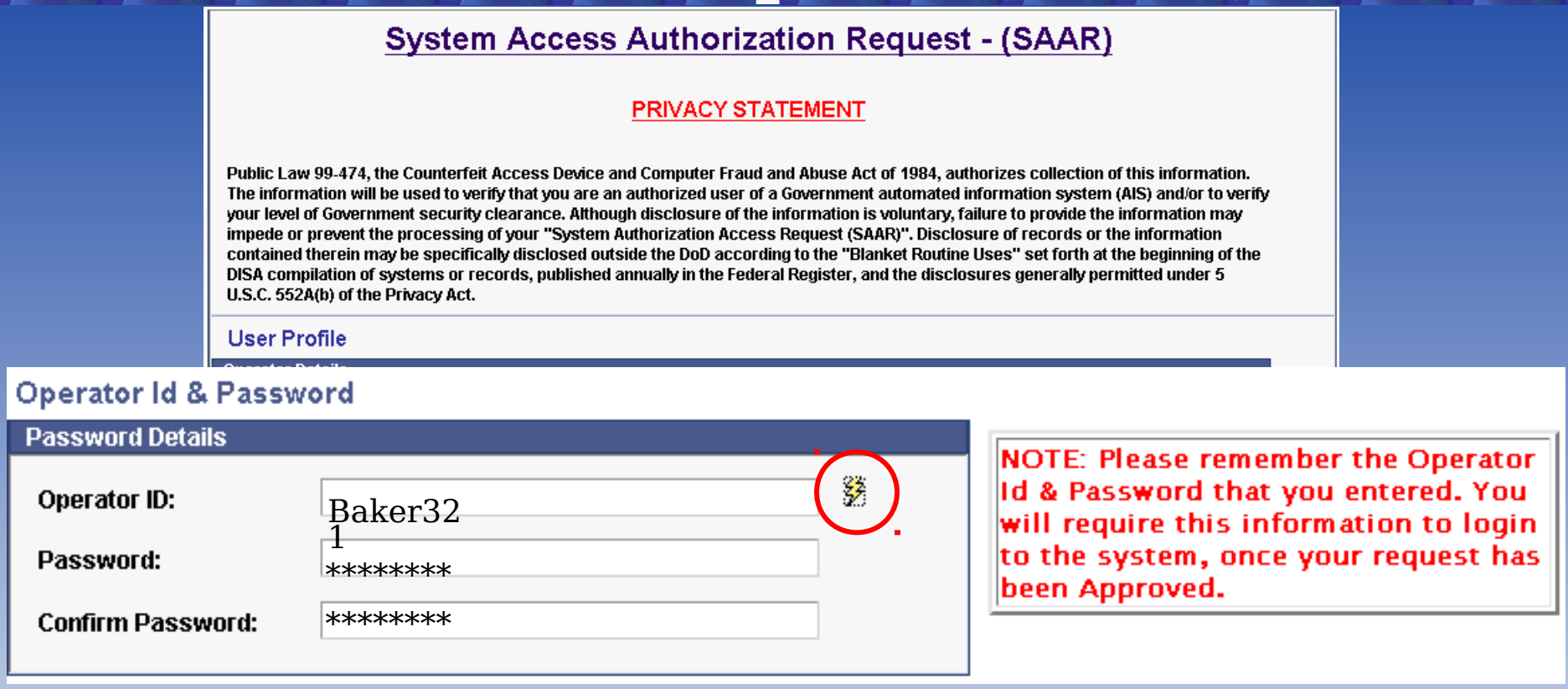
After review, the form will be sent to the Local NAM for approval

The SAAR will bypass the local NAM to the SUPER NAM if High level access is requested

The Initial NAM account will have to be submitted to the Super NAM for approval

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form


System Access Authorization Request - (SAAR)
PRIVACY STATEMENT
Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems or records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552A(b) of the Privacy Act.
User Profile
Operator Id & Password
Password Details
Operator ID:
Baker321
Password:
****
Confirm Password:
****
NOTE: Please remember the Operator Id & Password that you entered. You will require this information to login to the system, once your request has been Approved.

- The user will need to create an Operator Id and Password. In Client Server this was set up by the local SYSADM.
- The User will select the Operator Id/Password button to open the input panel
- The user can use the lighting bolt for the OprID to be computer generated or can self-create an OprID by using the guidelines.

Click to advance

Operator Id and Password Guidelines

Operator Id and Password Restrictions
- Operator Id is case sensitive and must be a minimum of 8 Characters Long not exceeding 25 characters.
- Operator Id can contain either Alpha-Numeric Character or Special Characters.
- Operator Id can be Generated Automatically by Clicking on the Lightning Bolt Icon next to the Operator Id Field.
- Operator Password must contain Alpha-Numeric Characters.
- Operator Password must be a minimum of 8 Characters Long not exceeding 25 characters.
- Operator Password must contain at least 2 digits.
- Operator Password must contain a mix of alpha characters and numbers.One Upper-case alpha and at least one lower case alpha.

- Operator Id
  - Minimum of 8 - max of 25 characters
  - Can contain alpha numeric characters
  - Can not be changed once established
  - **DO NOT USE PERIODS**

- Password
  - Must contain alpha numeric characters
  - Minimum of 8 - max of 25 characte
  - Must contain at least 2 numeric dig
  - Must contain at least one upper ca and one lower case alpha characte
  - **DO NOT USE PERIODS**

Once the Oprid and password are created click the OK button at the bottom of the page to return to the SAAR form

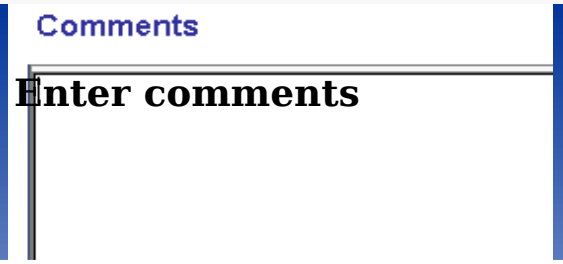
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont.

- General Attributes
  - SSN, Name, Rank/Rate and UIC are prefilled. Ensure this information is correct before continuing

- Input user's email and phone
  - Email must be .Mil or .Gov
  - The email is used for reporting the status of the process to the user

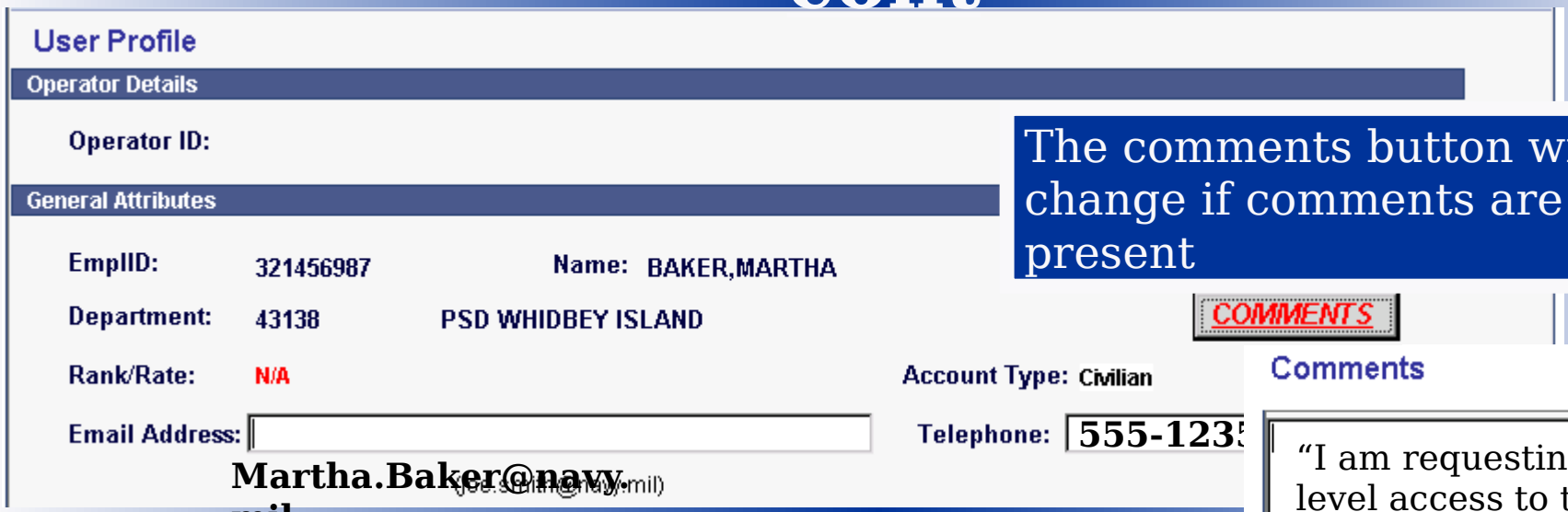
- The telephone entry is optional but is recommended should any questions arise from the form and the user needs to be contacted



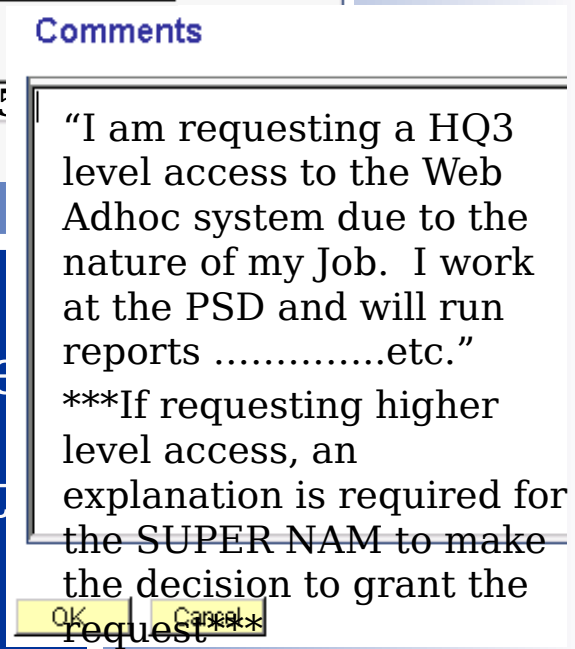
- Comments
  - Select the Comments button to have the comments box open for additional notes to be added

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont



The comments button will change if comments are present

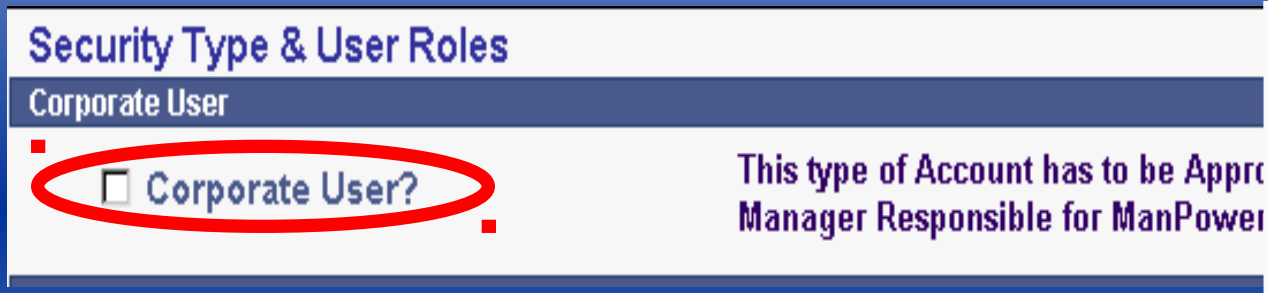

Comments
"I am requesting a HQ3 level access to the Web Adhoc system due to the nature of my Job. I work at the PSD and will run reports .....etc."
If requesting higher level access, an explanation is required for the SUPER NAM to make the decision to grant the request
OK
Cancel

- Comments
  - Comments **must** be entered if the user is requesting higher level access which requires the SAAR t be approved by the SUPER NAM
  - The SUPER NAM will reject a SAAR if there is no explanation for the high level access request

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont.

- Security Type and Role Users
  - The Supervisors and ISSO/FAMs must take extreme care not to allow users access to the wrong role type


Security Type & User Roles
Corporate User
Corporate User?
This type of Account has to be Appr
Manager Responsible for ManPower

- Corporate Users
  - Echelon level access

By checking this box, the user is requesting access to all records maintained by the NSIPS database. This can only be approved by the Super NAM at PERS-3. The Super NAM will be in charge of setting higher-level access accounts. If this box is checked the request will go to the Super NAM - NOT the local NAM – after SAAR Supervisor approval. This type of user should be limited to persons who need access to all records, for example, the NSIPS Helpdesk.

This gives access to the HR side of NSIPS ONLY - NOT WEB ADHOC.

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont.

- Security Type and Role Users
  - The Supervisors and ISSO/FAMs must take extreme care not to allow users access to the wrong role type

– Pay & Personnel Offices
  - PSD

Select to create HR accounts needing access to the ERM/NSIPS application in order to process transactions

– Command/Fleet Users
  - Admin Users, i.e. BUPERS, PSA, PLR

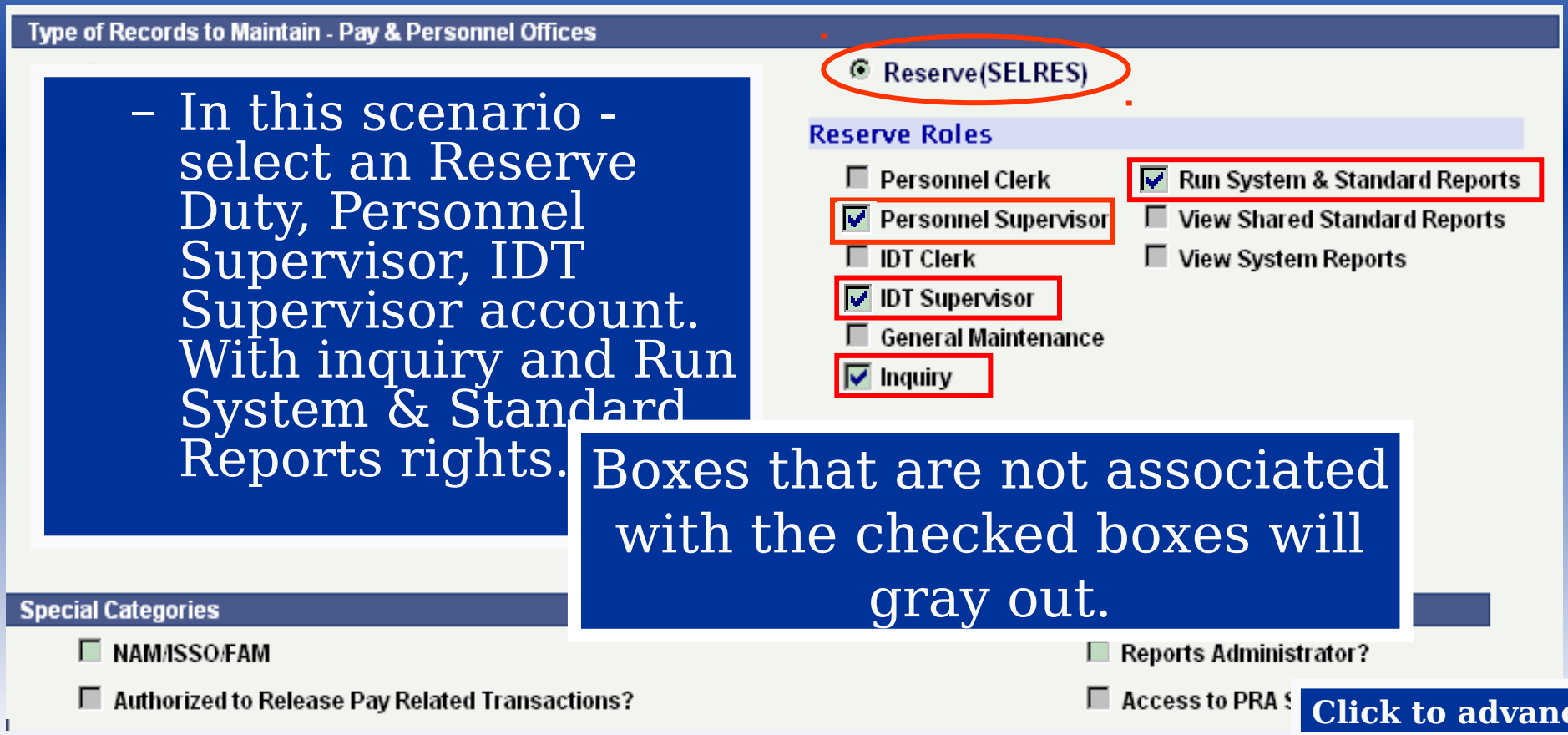
Select to create an Administrative type user. For example, a command PLR would be designated as a Cmd/Fleet User. This would give the user access to the ESR application

Command/Fleet Users will be further discussed later in the slide show.

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

- Select the appropriate roles and Special Categories
  - Choose either Active Duty or Reserve record access
  - Choose the appropriate function roles



- In this scenario - select an Reserve Duty, Personnel Supervisor, IDT Supervisor account. With inquiry and Run System & Standard Reports rights.

Boxes that are not associated with the checked boxes will gray out.

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont.

Establishing Special Categories

- There are 4 options that may be granted under Special Categories.
  - NAM/ISSO/FAM access will grant the user the ability to approve future local Pay and Personnel SAAR requests.
  - Authorized to Release Pay Related Transactions allows the user to release Pay related transactions. This is automatically defaulted for Pay Supervisors.
  - Reports Administrator will have the ability to manage reports to include the ability to setup reoccurring reports and delete reports
  - Access to PRA Sensitive Records allows the user to update accounts with Pay record accessibility

Not options for Reserves roles

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

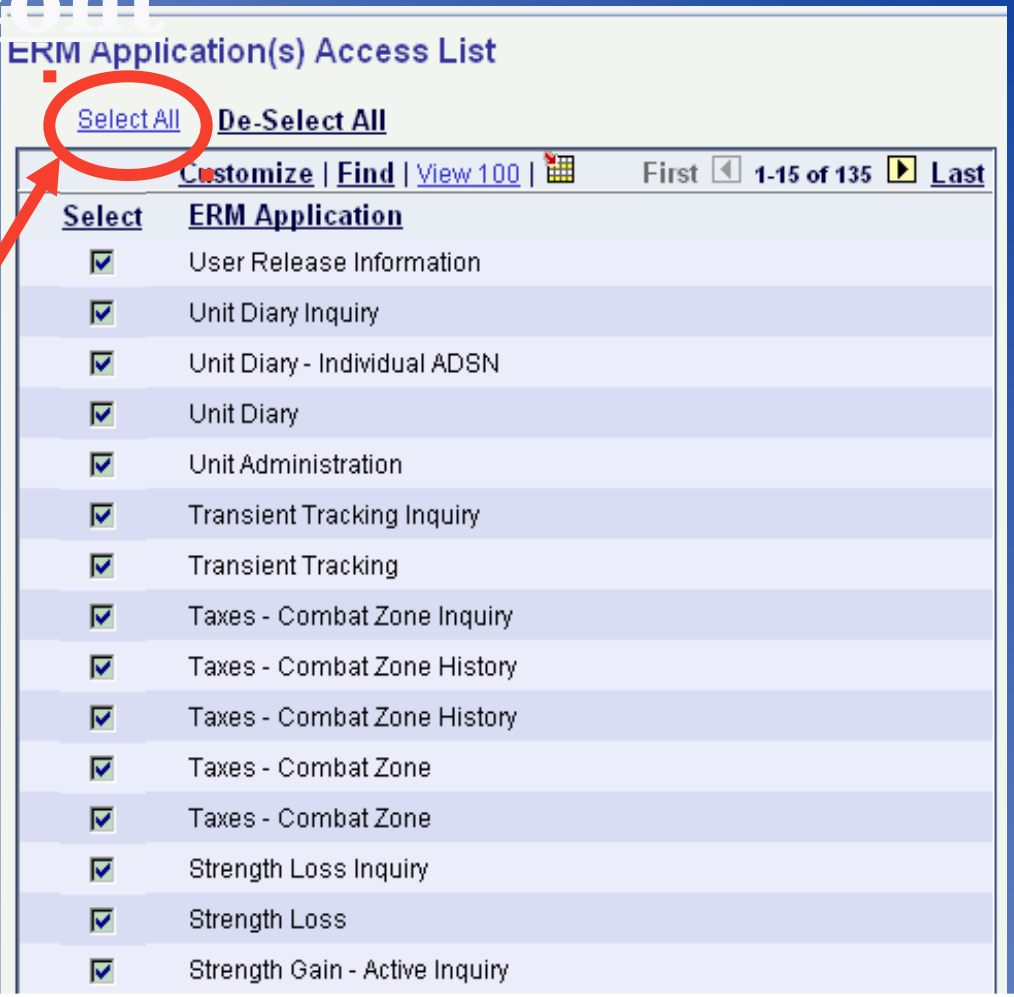
ERM Application Access List

This section has been added so the actions of users can be limited even further to specific functions.

Users can be limited to specific NSIPS functions by checking them under this section.

To give access to all functions select the 'Select All' button.

The choices will change based on the Role type selected. For example, Allotments will only



Coordinate subjects: For example – Gains must have address & phone, leave, dependency data etc., checked for the user to have access to all areas of the gain process.

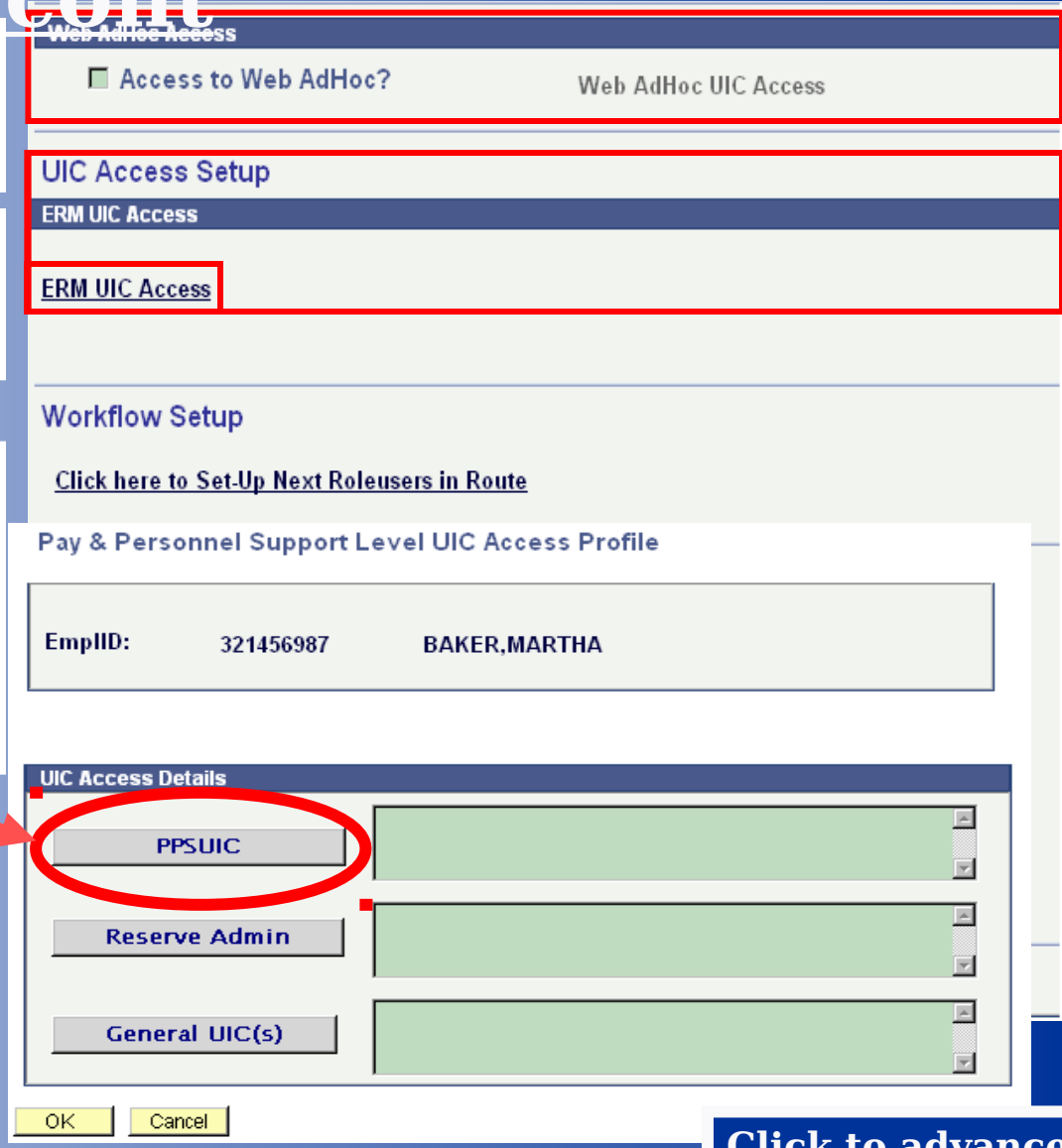
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Establishing UIC Access

- The ERM UIC Access link will open the UIC Access Details panel

- PPSUIC will grant access to all UICs that report to that UIC. For example– A PSD would input their UIC to have access to all UICs held by that PSD.



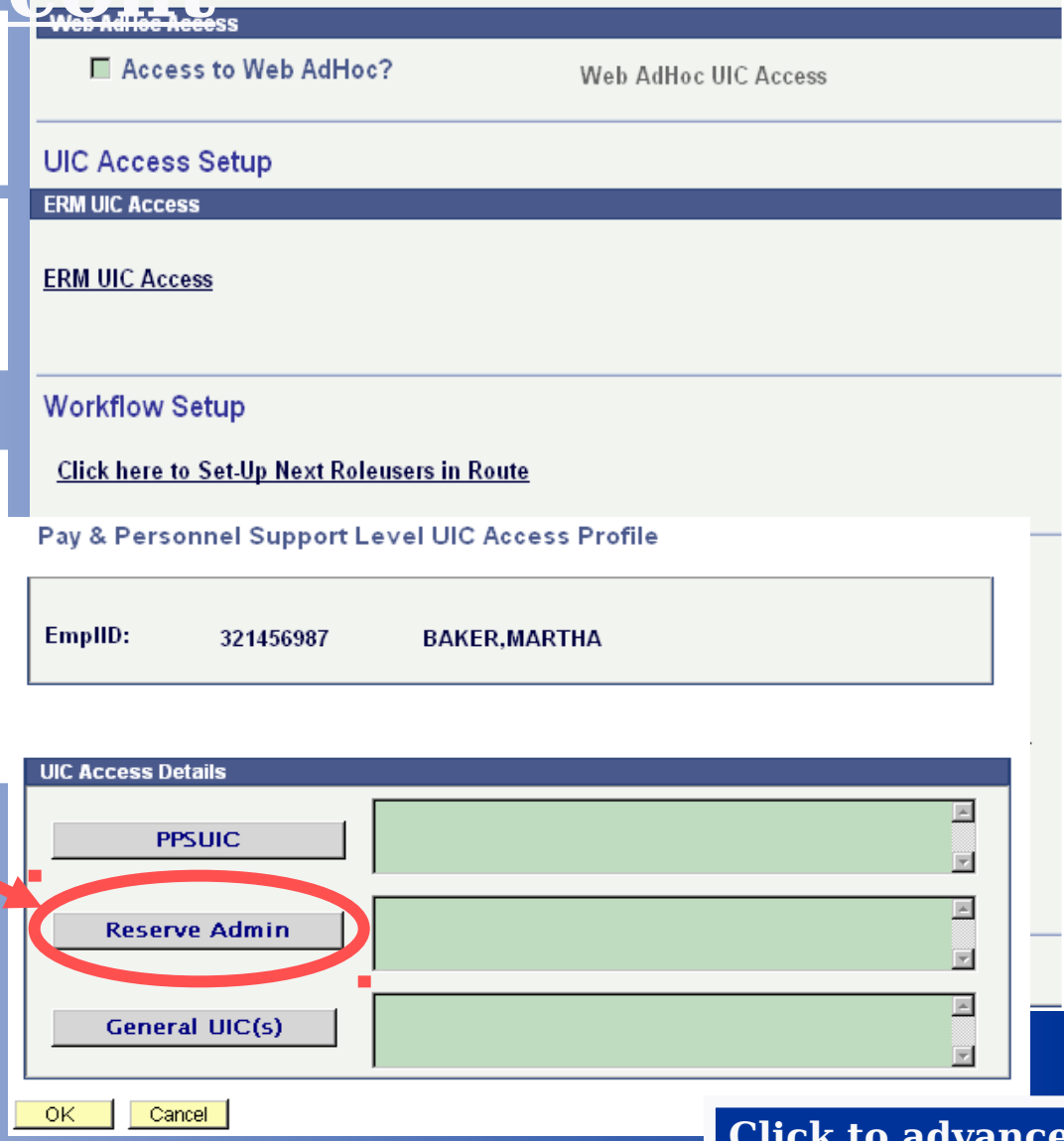
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Establishing UIC Access

- The ERM UIC Access link will open the UIC Access Details panel

- The Reserve Admin will be used for Reserve Commands.



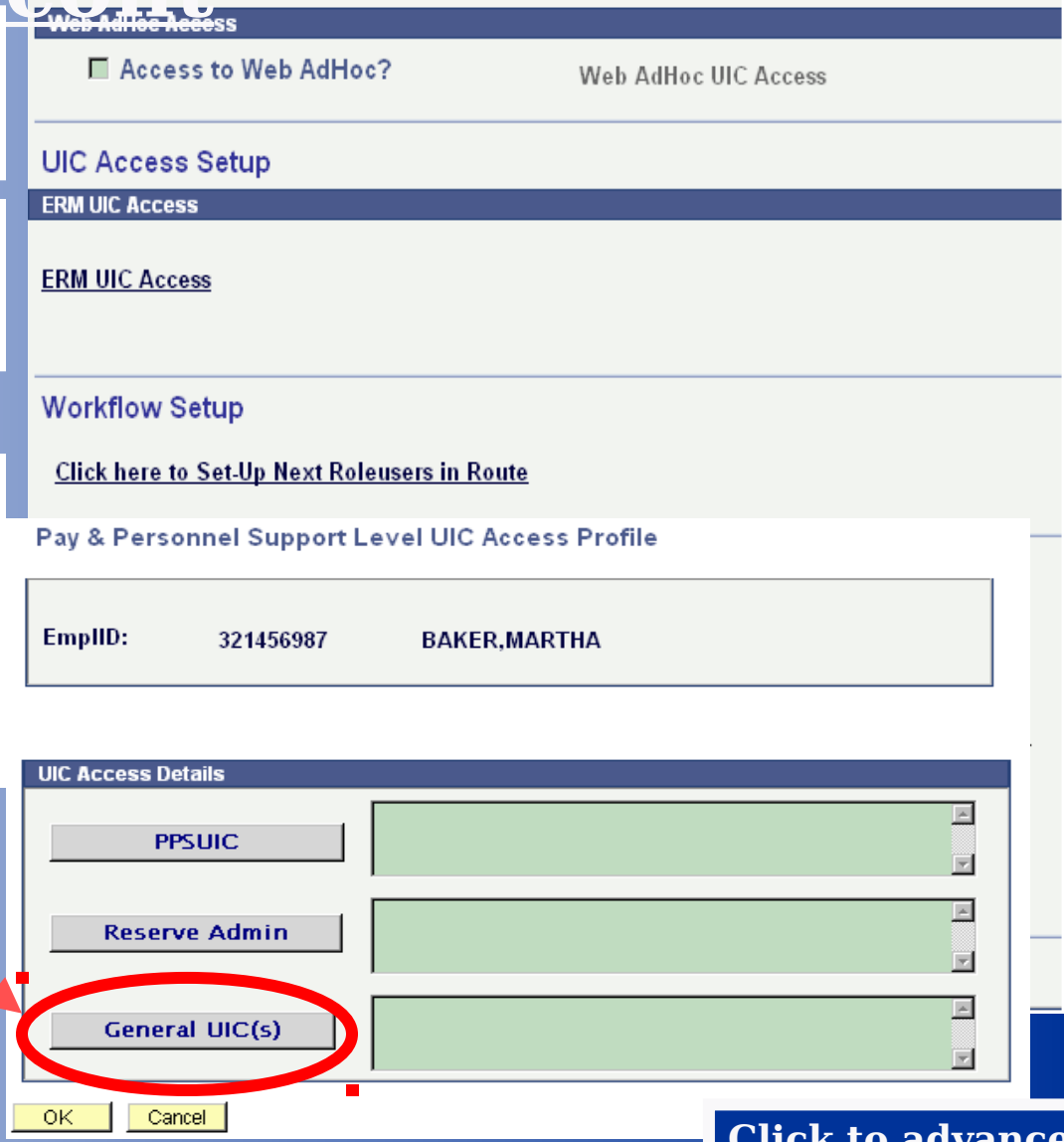
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Establishing UIC Access

- The ERM UIC Access link will open the UIC Access Details panel

- The General UIC(s) will limit access to the specific UICs listed.



Click to advance

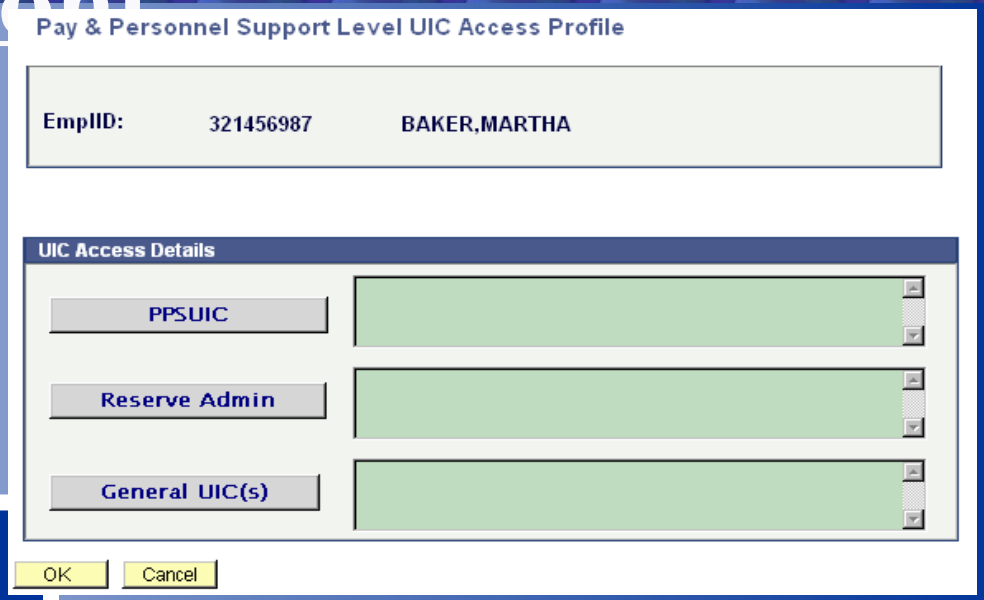
Filling Out the System Access Authorization Request (SAAR) Form, cont

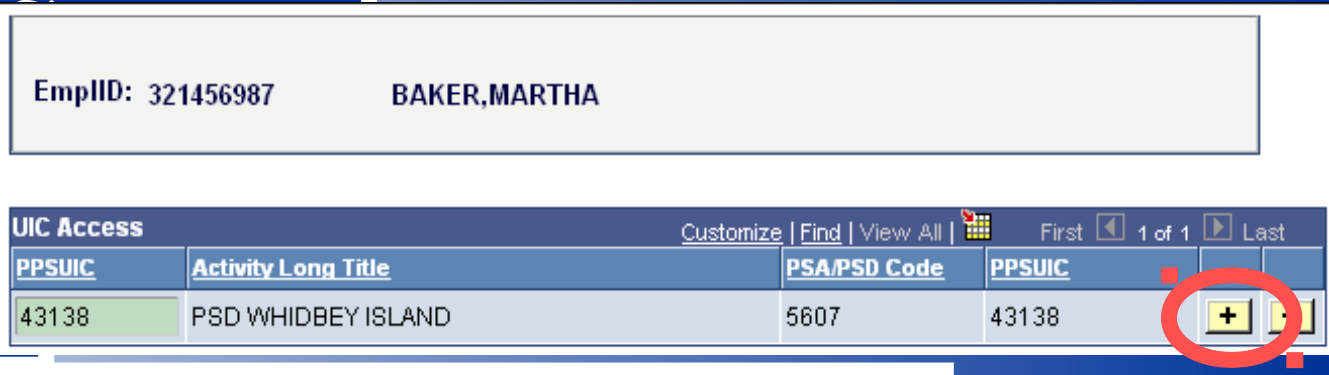
Establishing UIC Access

- After choosing the appropriate button the UIC Access input panel will appear.

- Enter the UIC(s) in this panel.
- Additional UICs can be added by using the Plus

- Access will be granted if approved by the FAM





UIC access for PPSUIC and Reserve Admin are limited to the UIC displayed at the start of the SAAR process

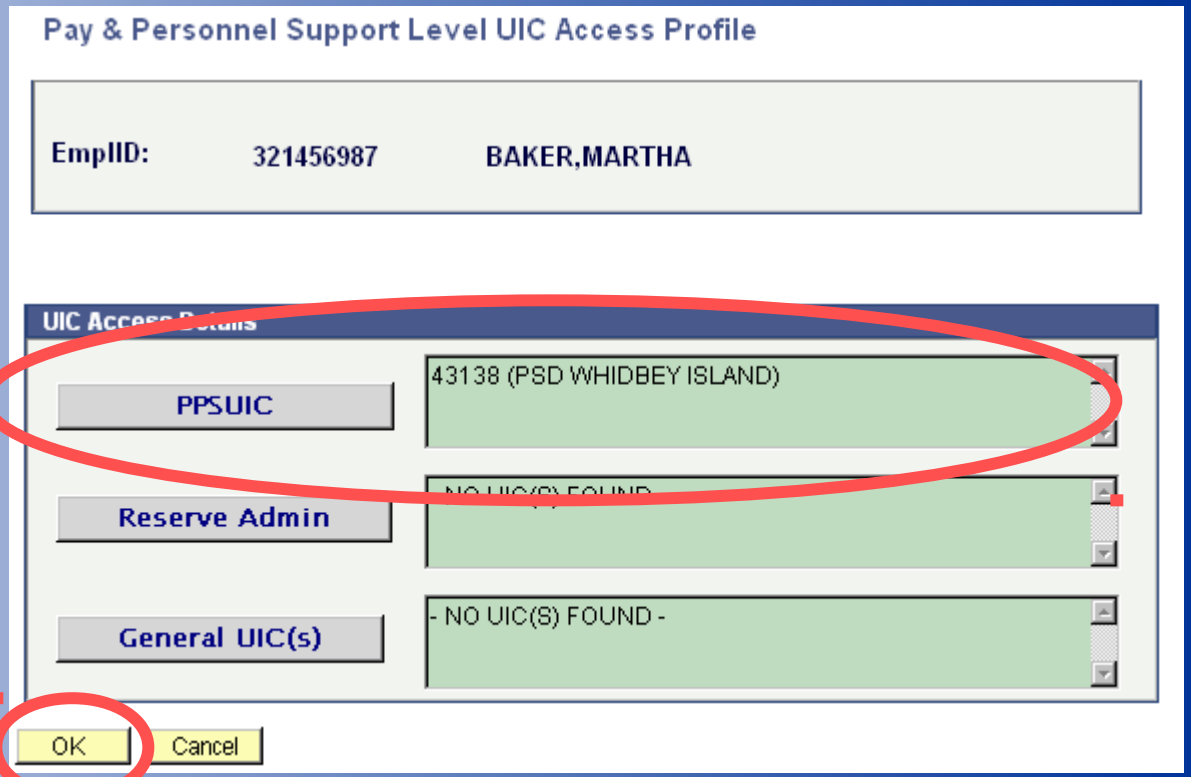
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Establishing UIC Access

After the user completes the ERM UIC input process, the UIC(s) and Command name(s) will appear in the areas next to the Access Button.

Select the OK button to close this panel and return to the SAAR

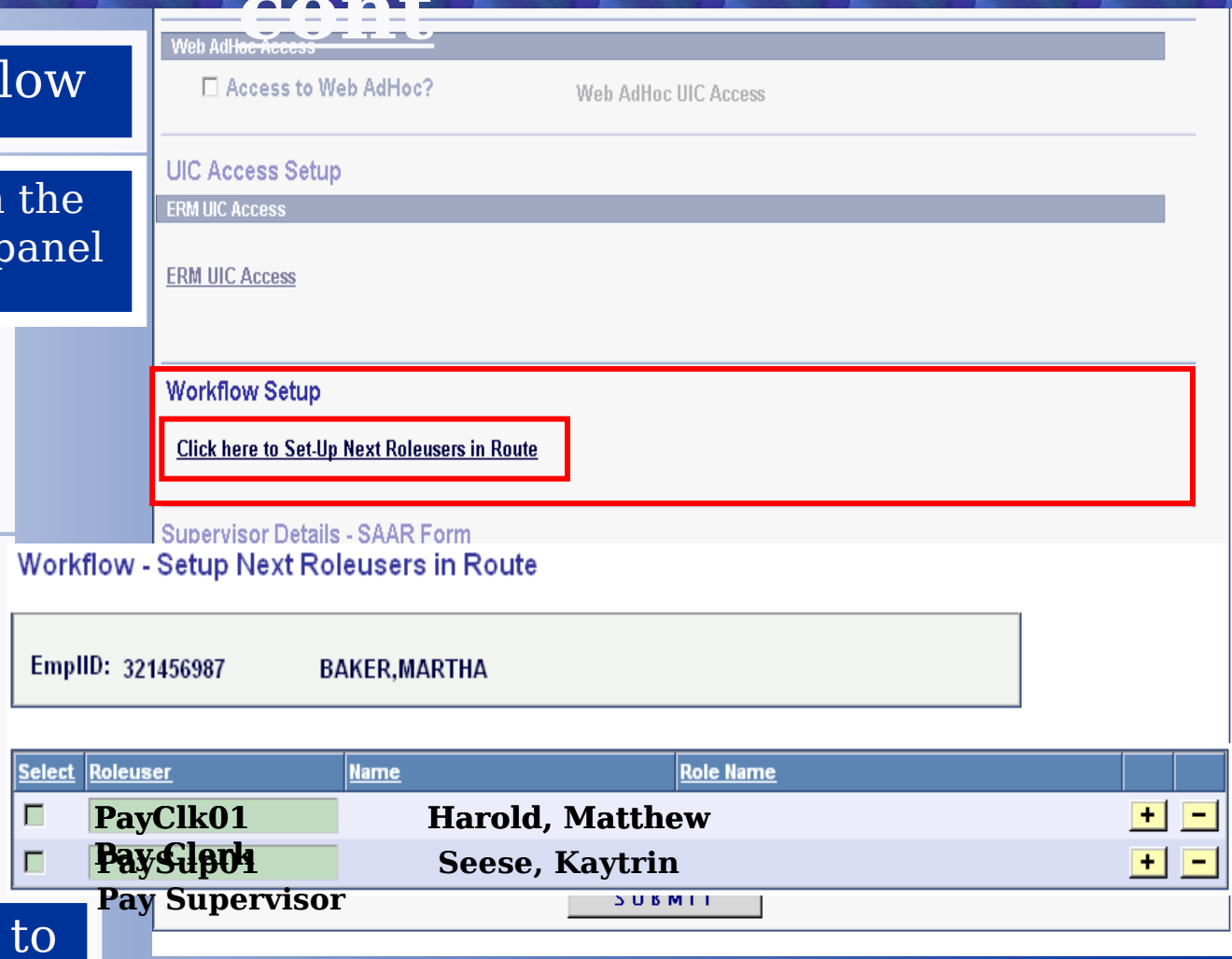


Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Creating user workflow

- Select the link to open the workflow setup input panel
- The user will enter the OprId of the Next in route Roleuser
- A search function does not exist, so the user must know the correct Operator Id to input.
- If multiple Id's are to be added, do this by clicking the plus sign

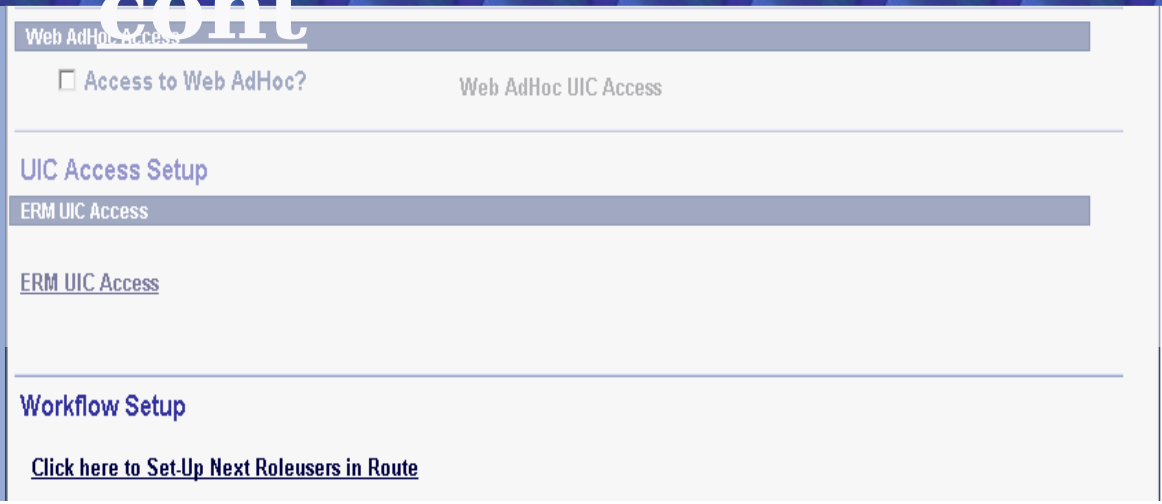


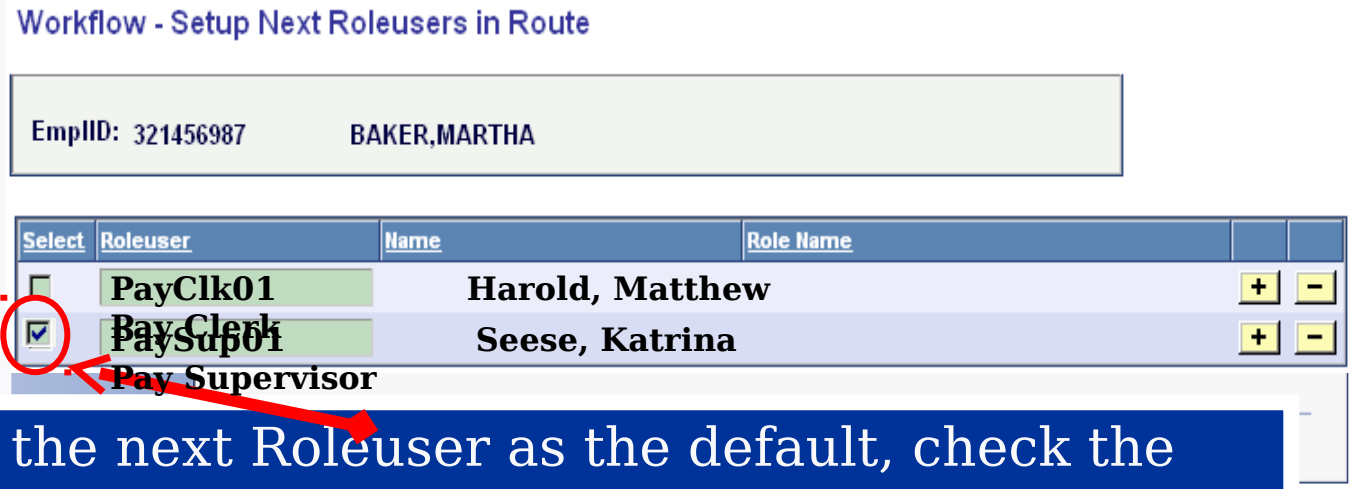
Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Creating user workflow

- The same 4 tier workflow still applies. Pers Clerk to Pers Sup - Pers Sup to Pay Clerk - Pay Clerk to Pay Sup.
- This can be modified to meet the needs of the command





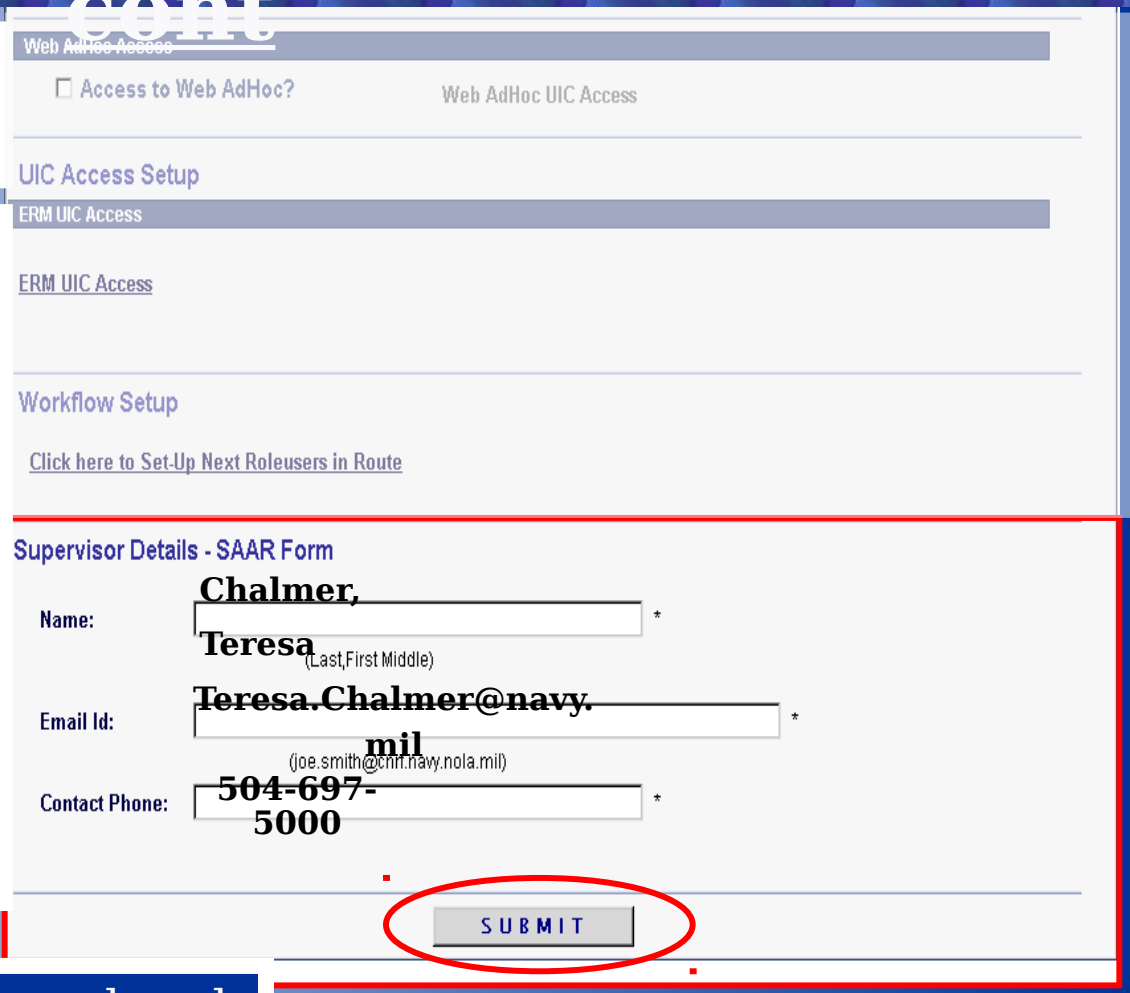
To set the next Roleuser as the default, check the box. This person will automatically be chosen as the next person to route the workflow to. Select the OK button to close this panel.

Click to advance

Filling Out the System Access Authorization Request (SAAR) Form, cont

Supervisor Details

- The user MUST ensure the information is entered correctly. This form will be emailed to the email listed, which is a very important step in the approval process.
- The supervisor must enter the information exactly as it appears here in order for the approval process to begin



- Once the information is entered and verified select the SUBMIT button to submit the form for approval

Click to advance

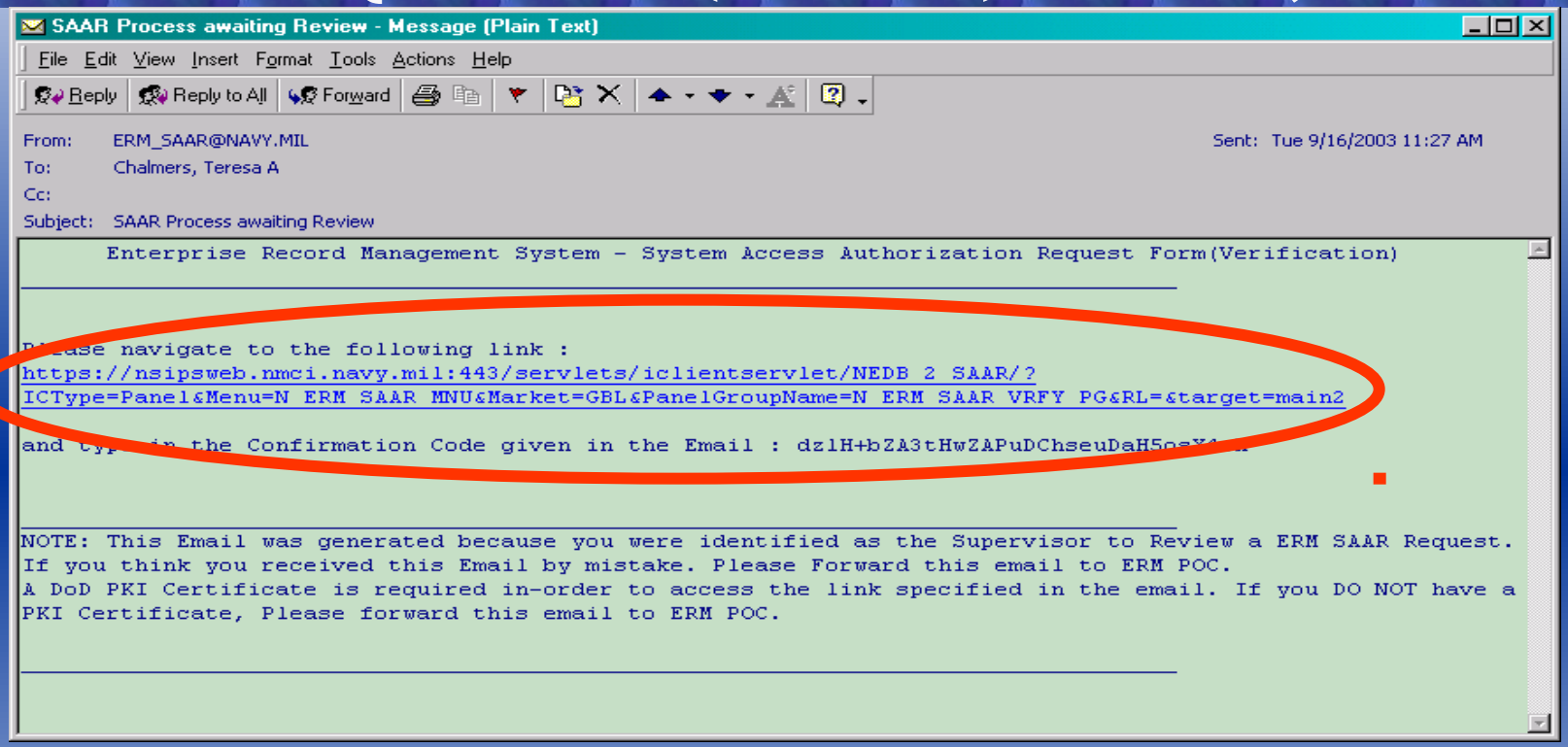
Filling Out the System Access Authorization Request (SAAR) Form, cont

This concludes the SAAR submission process.

Next will be The SAAR Supervisor function

Click to advance

SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont


SAAR Process awaiting Review - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: ERM_SAAR@NAVY.MIL
Sent: Tue 9/16/2003 11:27 AM
To: Chalmers, Teresa A
Cc:
Subject: SAAR Process awaiting Review

Enterprise Record Management System - System Access Authorization Request Form(Verification)

Please navigate to the following link :
https://nsipsweb.nmci.navy.mil:443/servlets/iclientservlet/NEDB_2_SAAR/?ICType=Panel&Menu=N_ERM_SAAR_MNU&Market=GBL&PanelGroupName=N_ERM_SAAR_VRFY_PG&RL=&target=main2

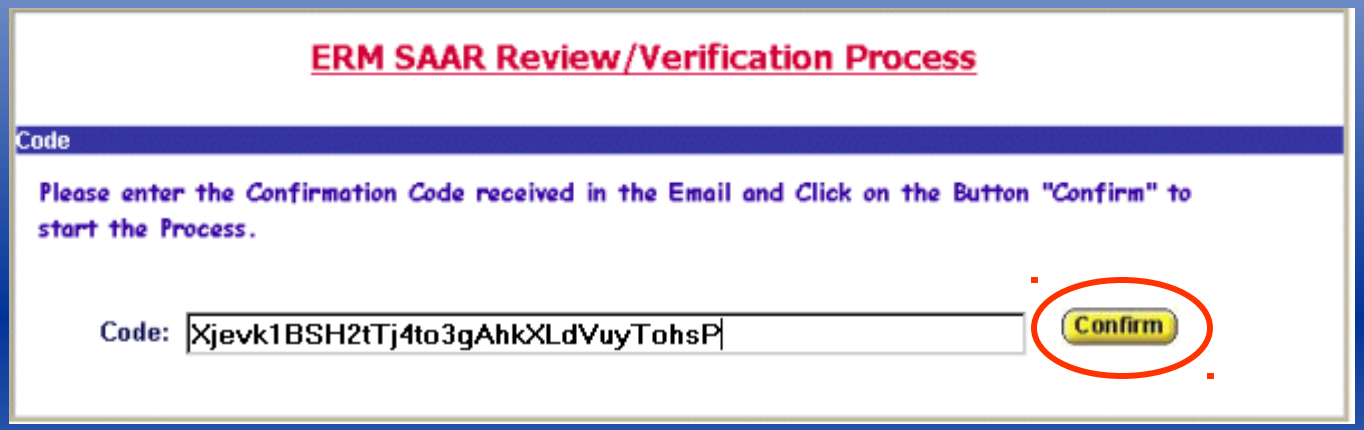
and type in the Confirmation Code given in the Email : dzlH+bZA3tHwZAPuDChseuDaH5oaY4

NOTE: This Email was generated because you were identified as the Supervisor to Review a ERM SAAR Request.
If you think you received this Email by mistake. Please Forward this email to ERM POC.
A DoD PKI Certificate is required in-order to access the link specified in the email. If you DO NOT have a PKI Certificate, Please forward this email to ERM POC.

- The Supervisor will receive an email similar to this.
- The subject line will be SAAR Process Awaiting Review
- This email will contain a confirmation code.
- The supervisor will copy the code and click the hyper-link to bring up the confirm screen.

Click to advance

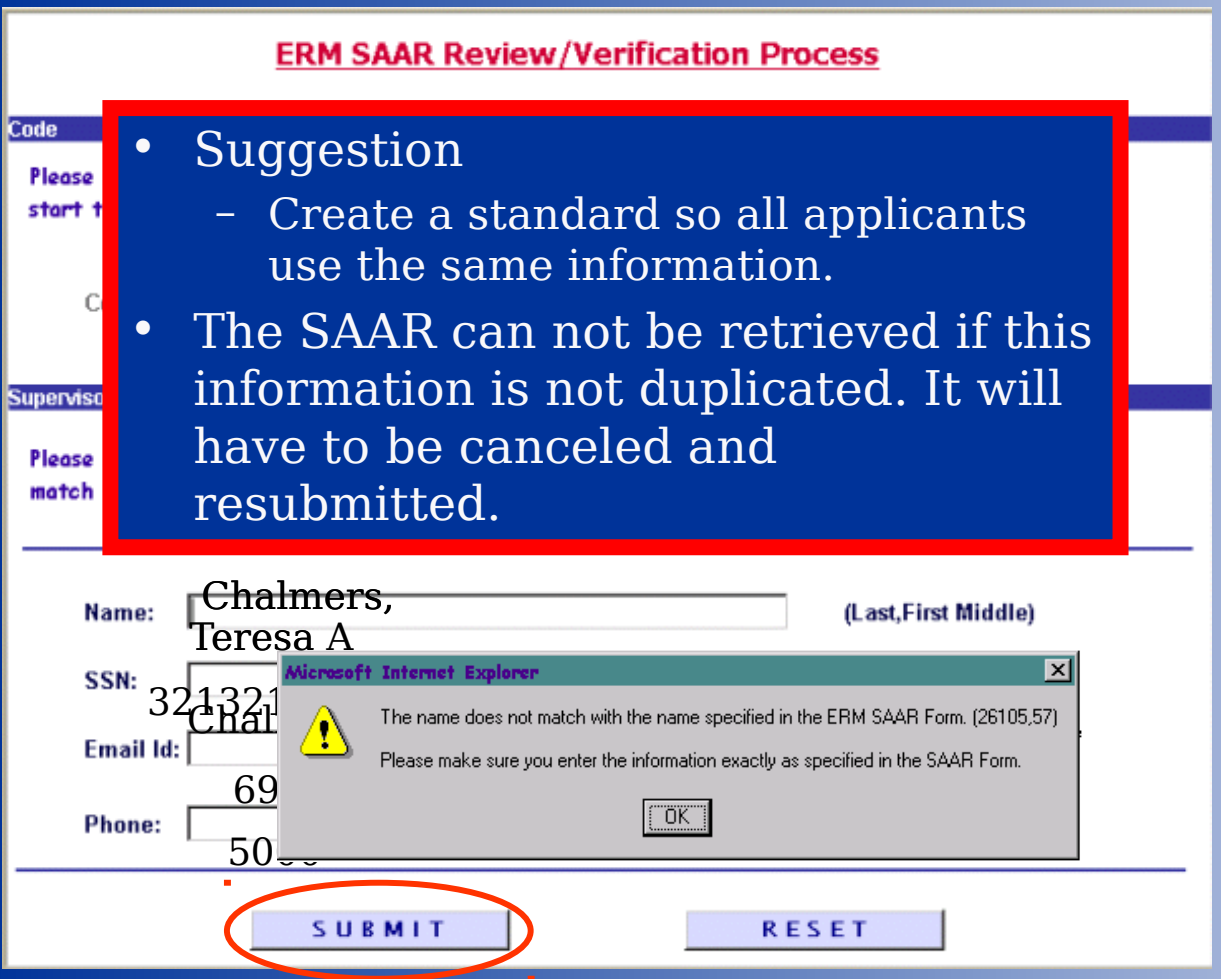
SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont


ERM SAAR Review/Verification Process
Code
Please enter the Confirmation Code received in the Email and Click on the Button "Confirm" to start the Process.
Code:
Xjevk1BSH2tTj4to3gAhkXLdVuyTohsP
Confirm

- The link will open to a web page similar to this
- The supervisor will paste the confirmation code in the text box
- Then confirm the code by clicking on the confirm button

Click to advance

SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont

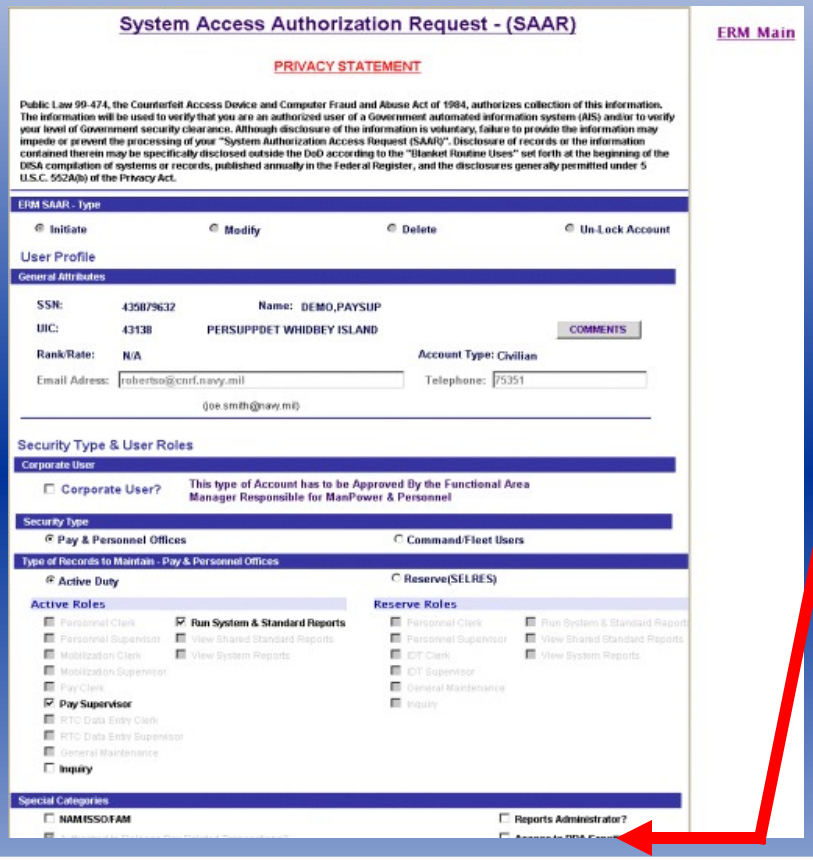


- Suggestion
  - Create a standard so all applicants use the same information.
- The SAAR can not be retrieved if this information is not duplicated. It will have to be canceled and resubmitted.

- **The Supervisor Details panel will appear after the supervisor selects the Confirm button**
- **The SAAR Supervisor will input their information**
- **An error is received if the data entered here does not match exactly to what the requester entered**
- **Use the Submit button to open the submitted SAAR form**

Click to advance

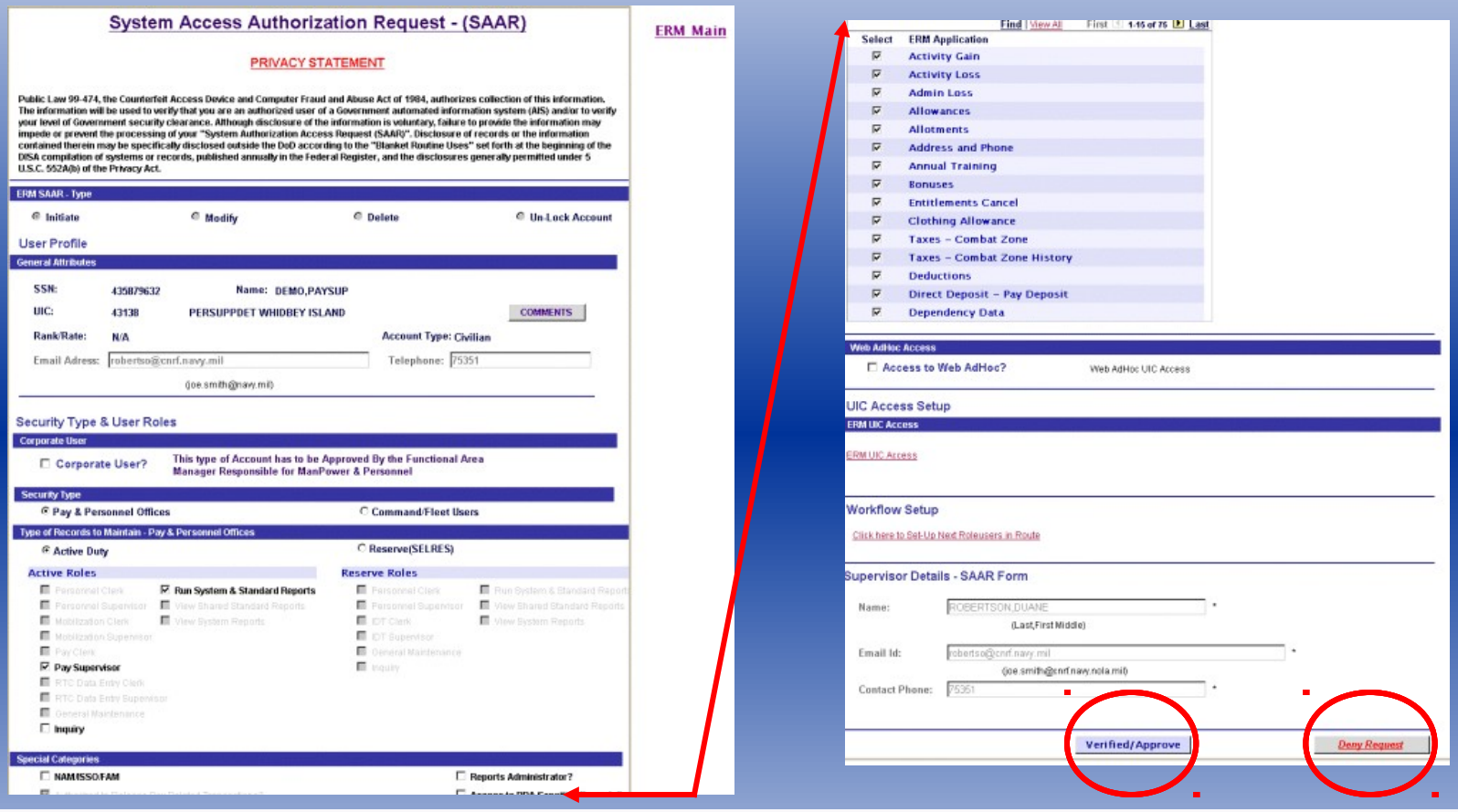
SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont


System Access Authorization Request - (SAAR)
ERM Main
PRIVACY STATEMENT
Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems or records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552A(b) of the Privacy Act.
ERM SAAR - Type
Initiate
Modify
Delete
Un-Lock Account
User Profile
General Attributes
SSN: 435879632
Name: DEMO,PAYSUP
UIC: 43138
PERSUPPDET WHIDBEY ISLAND
COMMENTS
Rank/Rate: N/A
Account Type: Civilian
Email Adress: robertso@cnrf.navy.mil
Telephone: 75351
(joe.smith@navy.mil)
Security Type & User Roles
Corporate User
Corporate User?
This type of Account has to be Approved By the Functional Area Manager Responsible for ManPower & Personnel
Security Type
Pay & Personnel Offices
Command/Fleet Users
Type of Records to Maintain - Pay & Personnel Offices
Active Duty
Reserve(SELRES)
Active Roles
Run System & Standard Reports
Pay Supervisor
Inquiry
Reserve Roles
Special Categories
NAM/ISSO/FAM
Reports Administrator?

- There are 2 steps to the verifying/approval process. The first being the SAAR Supervisor and the second being the FAM/ISSO/NAM.
- Again, the SAAR Supervisor does not need to have an NSIPS account just a valid .Mil or .Gov email account.

Click to advance

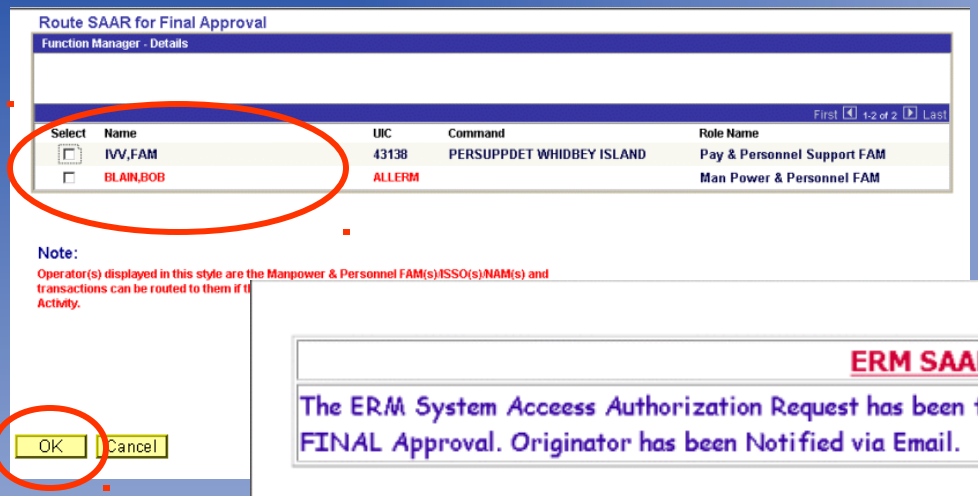
SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont


System Access Authorization Request - (SAAR)
ERM Main
PRIVACY STATEMENT
Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)". Disclosure of records or the information contained therein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems or records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552A(b) of the Privacy Act.
ERM SAAR - Type
Initiate
Modify
Delete
Un-Lock Account
User Profile
General Attributes
SSN: 435879632
Name: DEMO,PAYSUP
UIC: 43138
PERSUPPDET WHIDBEY ISLAND
COMMENTS
Rank/Rate: N/A
Account Type: Civilian
Email Adress: robertso@cnrf.navy.mil
Telephone: 75351
(joe.smith@navy.mil)
Security Type & User Roles
Corporate User
Corporate User?
This type of Account has to be Approved By the Functional Area Manager Responsible for ManPower & Personnel
Security Type
Pay & Personnel Offices
Command/Fleet Users
Type of Records to Maintain - Pay & Personnel Offices
Active Duty
Reserve(SELRES)
Active Roles
Run System & Standard Reports
Pay Supervisor
Inquiry
Reserve Roles
Special Categories
NAMISSO/FAM
Reports Administrator?
Find | View All
First 1-15 of 75 Last
Select
ERM Application
Activity Gain
Activity Loss
Admin Loss
Allowances
Allotments
Address and Phone
Annual Training
Bonuses
Entitlements Cancel
Clothing Allowance
Taxes – Combat Zone
Taxes – Combat Zone History
Deductions
Direct Deposit – Pay Deposit
Dependency Data
Web AdHoc Access
Access to Web AdHoc?
Web AdHoc UIC Access
UIC Access Setup
ERM UIC Access
ERM UIC Access
Workflow Setup
Click here to Set-Up Next Roleusers in Route
Supervisor Details - SAAR Form
Name:
ROBERTSON,DUANE
(Last,First Middle)
Email Id:
robertso@cnrf.navy.mil
(joe.smith@cnrf.navy.nola.mil)
Contact Phone:
75351
Verified/Approve
Deny Request

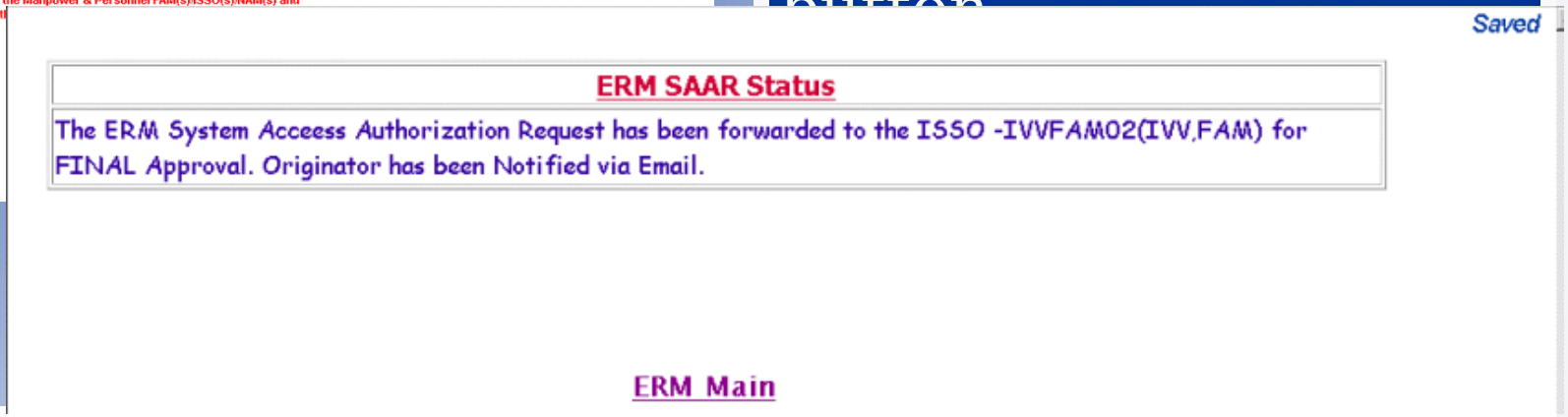
- Click the Deny button if a SAAR is to be denied. An email is sent to the user with the explanation as to why the SAAR was denied.

Click to advance

SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) Form, Cont



Select the NSIPS Area Manager (NAM) to route to, select the OK button


Saved
ERM SAAR Status
The ERM System Acceess Authorization Request has been forwarded to the ISSO -IVVFAM02(IVV,FAM) for FINAL Approval. Originator has been Notified via Email.
ERM Main

- The Supervisor will now route the SAAR form to the Local NAM, which will be the final approval
- The above confirmation is received, and an email is sent to the Originator
- The SAAR is now in the final stage of the approval process

Click to advance

Next Will Be the Corporate and Fleet/Command Users

Click here to continue to the next slide of this presentation.

Click here to bypass this section and move to the Web Ad Hoc section

Click here to bypass the Corporate and Fleet/Command Users and the Web Ad Hoc sections of the presentation. This link will direct the user to Forgotten Passwords section

Corporate -SAAR

- A Corporate User can be assigned to either a Pay and Personnel Office User or Fleet/Command User.
- Provides the user access to all records that are maintained in the NSIPS Database.
- Highest level of user access available, and should be granted with extreme caution.

Security Type & User Roles
Corporate User
Corporate User?
This type of Account has to be Approved By the Functional Area Manager Responsible for ManPower & Personnel

Click to advance

Corporate -SAAR

- Examples of a user with this type of access
  - BUPERS
  - NSIPS/ESR Help Desk
- To request a Corporate account check the box next to “Corporate User”

Security Type & User Roles
Corporate User
Corporate User?
This type of Account has to be Approved By the Functional Area Manager Responsible for ManPower & Personnel

Click to advance

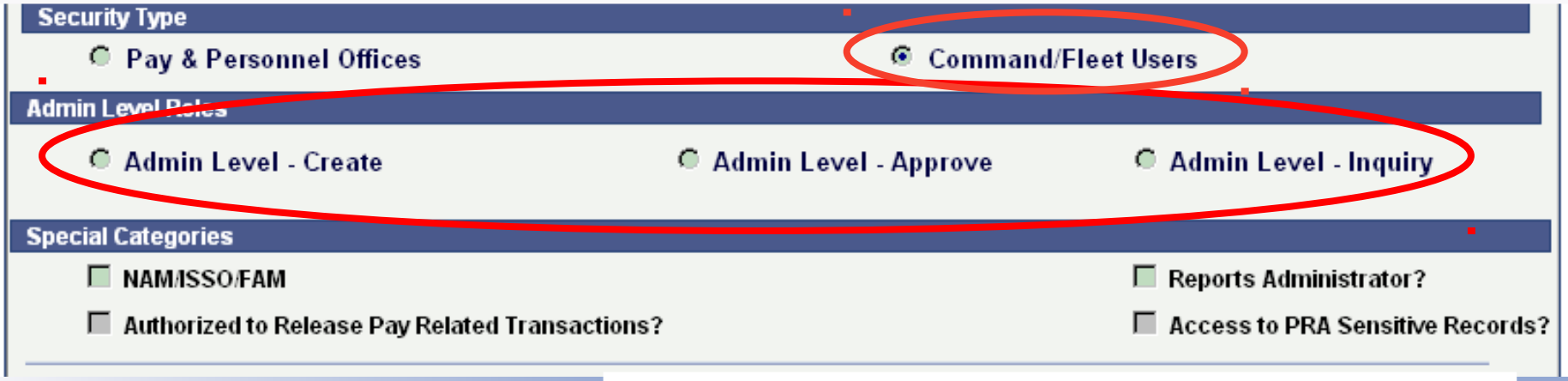
Corporate -SAAR

- The routing of the corporate SAAR is different than a regular SAAR
- The user submits the request to the SAAR Supervisor
- After review, it will be submitted to the SUPER NAM, **NOT the Local NAM**

Click to advance

Fleet/Command -SAAR

Click the Command/Fleet Users radio button to create Admin Role users



- **Three levels of Access**
  - **Create**
  - **Approve**
  - **Inquiry**

- Create level accounts will create transactions related to ESR.
- Approve Level would release the transactions,
- Inquiry is for view access only.

Click to advance

Fleet/Command -SAAR

- **Special Categories**
  - **NAM/ISSO/FAM**
  - **Reports Administrator**

Just as the Pay and Personnel Offices' roles, The NAM/ISSO/FAM and Reports Administrator are options the Command/Fleet Users can choose.

Click to advance

Fleet/Command -SAAR

- The ERM Application for Fleet/Command Users allows the user access to ESR type transactions
- Create or Approve accounts can have access to all ESR functions
- Can be limited even further by checking only the applications the user will need

Fleet/Command -SAAR

- Inquiry accounts are limited to General ESR inquiry only

Click to advance

Fleet/Command -SAAR

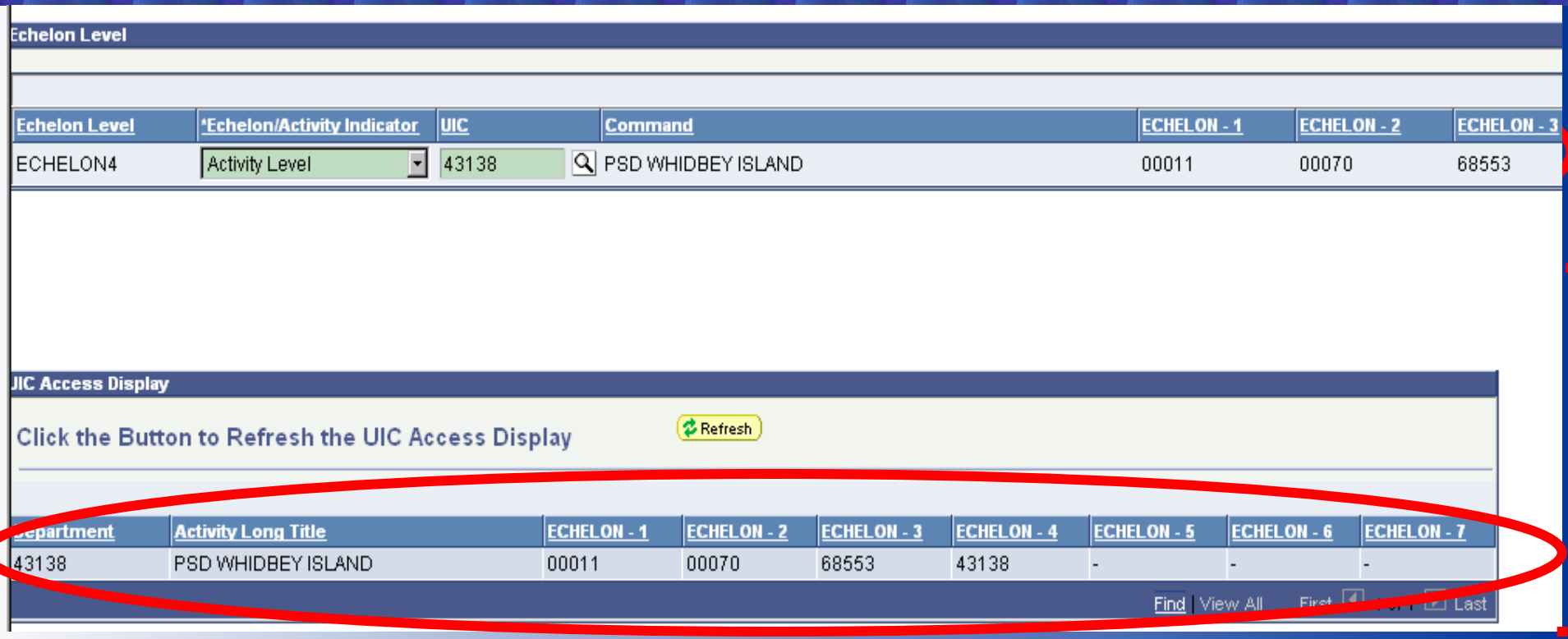
- The user will click on the ERM UIC Access Button to open the Administrative UIC Access Profile

- In this panel UIC permissions will be granted

- There are 2 levels of Access for Fleet Users
  - Activity
    - Allows access to only the UIC(s) listed

Click to advance

Fleet/Command -SAAR



The Activity level allows access to records that belong to that particular UIC.

The UIC Access Display shows only the chosen UICs

Click to advance

Fleet/Command -SAAR

Echelon Level

Echelon Level	*Echelon/Activity Indicator	UIC	Command	ECHELON - 1	ECHELON - 2	ECHELON - 3
ECHELON3	Echelon Level	68553	PERSONNEL SUPPORT ACTY WEST	00011	00070	68553

- The user will click on the ERM UIC Access Button to open the Administrative UIC Access Profile
- In this panel UIC permissions will be granted
- There are 2 levels of Access for Fleet Users
  - Activity
    - Allows access to only the UIC(s) listed
  - Echelon
    - Allows access to all UIC(s) that report to the UIC(s) listed

Click to advance

Fleet/Command -SAAR

Echelon Level

Echelon Level	*Echelon/Activity Indicator	UIC	Command	ECHELON - 1	ECHELON - 2	ECHELON - 3
ECHELON3	Echelon Level	68553	PERSONNEL SUPPORT ACTY WEST	00011	00070	68553

UIC Access Display

Click the Button to Refresh the UIC Access Display

Refresh

Department	Activity Long Title	ECHELON - 1	ECHELON - 2	ECHELON - 3	ECHELON - 4	ECHELON - 5	ECHELON - 6	ECHELON - 7
42817	PSD ASWTRACEN	00011	00070	68553	42817			
42827	PSD NORTH ISLAND	00011	00070	68553	42827			
42828	PSD CORONADO	00011	00070	68553	42828			
43053	PSD DENVER	00011	00070	68553	43053			
43073	PERSONEL SUPT ACTY NAVPOSGRADS	00011	00070	68553	43073			
43075	PERSONNEL SUPT ACTY DET FALLON	00011	00070	68553	43075			
43077	PERSONNEL SUP ACTY DET NAS LEM	00011	00070	68553	43077			
43118	PSD CAMP PENDLETON	00011	00070	68553	43118			
43136	PERSONNEL SUP ACTY DET EVERETT	00011	00070	68553	43136			
43137	PSD BREMERTON	00011	00070	68553	43137			
43138	PSD WHIDBEY ISLAND	00011	00070	68553	43138			
43144	PERSONNEL SUPT ACTY DET CHLAKE	00011	00070	68553	43144			
43146	PERSONNEL SUPT ACTY DET PHEU	00011	00070	68553	43146			
43150	PSD BANGOR	00011	00070	68553	43150			
43307	PERSONNEL SUPT ACTY DET ELCENT	00011	00070	68553	43307			
44584	CSD YUMA	00011	00070	68553	43307	44584	-	-
45091	CUSTOMER SERV DESK TWENTY NINE	00011	00070	68553	43118	45091	-	-
48444	CSD COLORADO	00011	00070	68553	43053	48444	-	-
49330	PERSONNEL SUPT ACTY DET OKLA	00011	00070	68553	49330	-	-	-
49756	CSD FT HUACHUCA	00011	00070	68553	43307	49756	-	-

Find | View

The Echelon level will grant access to all UICs that report to the UIC of choice

Click to advance

Fleet/Command -SAAR

The routing of the Fleet/Command SAAR also has the two step approval process. Starting with a SAAR Supervisor and ending with a NAM that has Fleet Command User approval authority.

At this time All Command/Fleet Users request must be routed to PERS-3/Super NAM for approval

Click to advance

Next Segment is Web Adhoc

If Web Adhoc will not be used Click Here to advance to Forgotten Passwords segment

Click Here to advance to the Web Adhoc segment

SAAR - Web Adhoc

- Must be submitted and approved in order to process Adhoc Reports
- On the SAAR form check the box next to ‘Access to Web Adhoc?’
- This will activate the link. Click the ‘Web Adhoc UIC Access’ Link

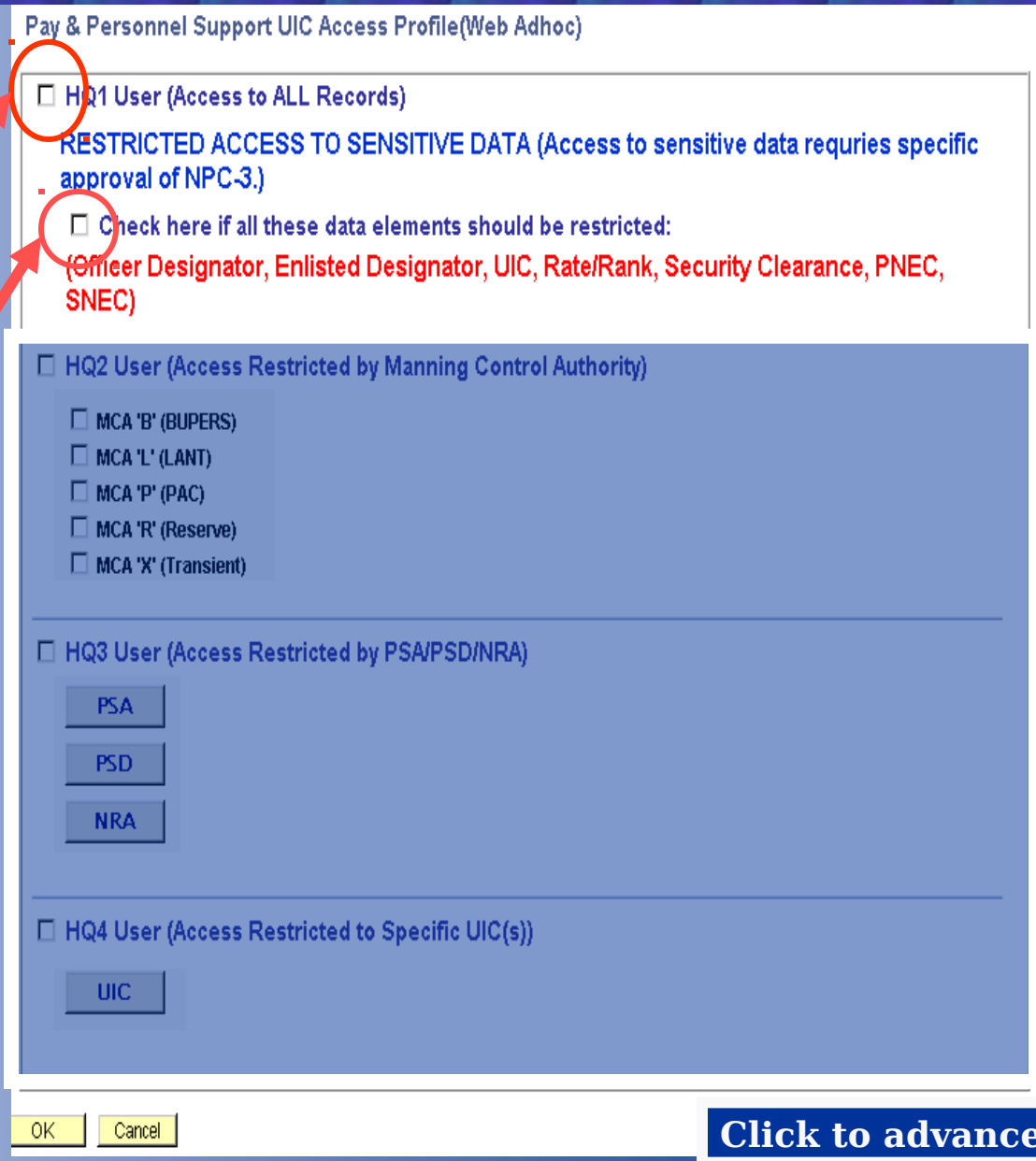
It is recommended that ALL personnel select this option if access to WEB Adhoc is needed. This will alleviate the duplication of initial SAAR forms generated.

Click to advance

SAAR - Web Adhoc

Four levels to Web Adhoc

- HQ1 is the highest level of access in Web Adhoc
  - Queried information can be limited
  - This will remove the ability to run queries based on sensitive information, such as Designators, UIC, Rank/Rate, NEC, and Clearance.

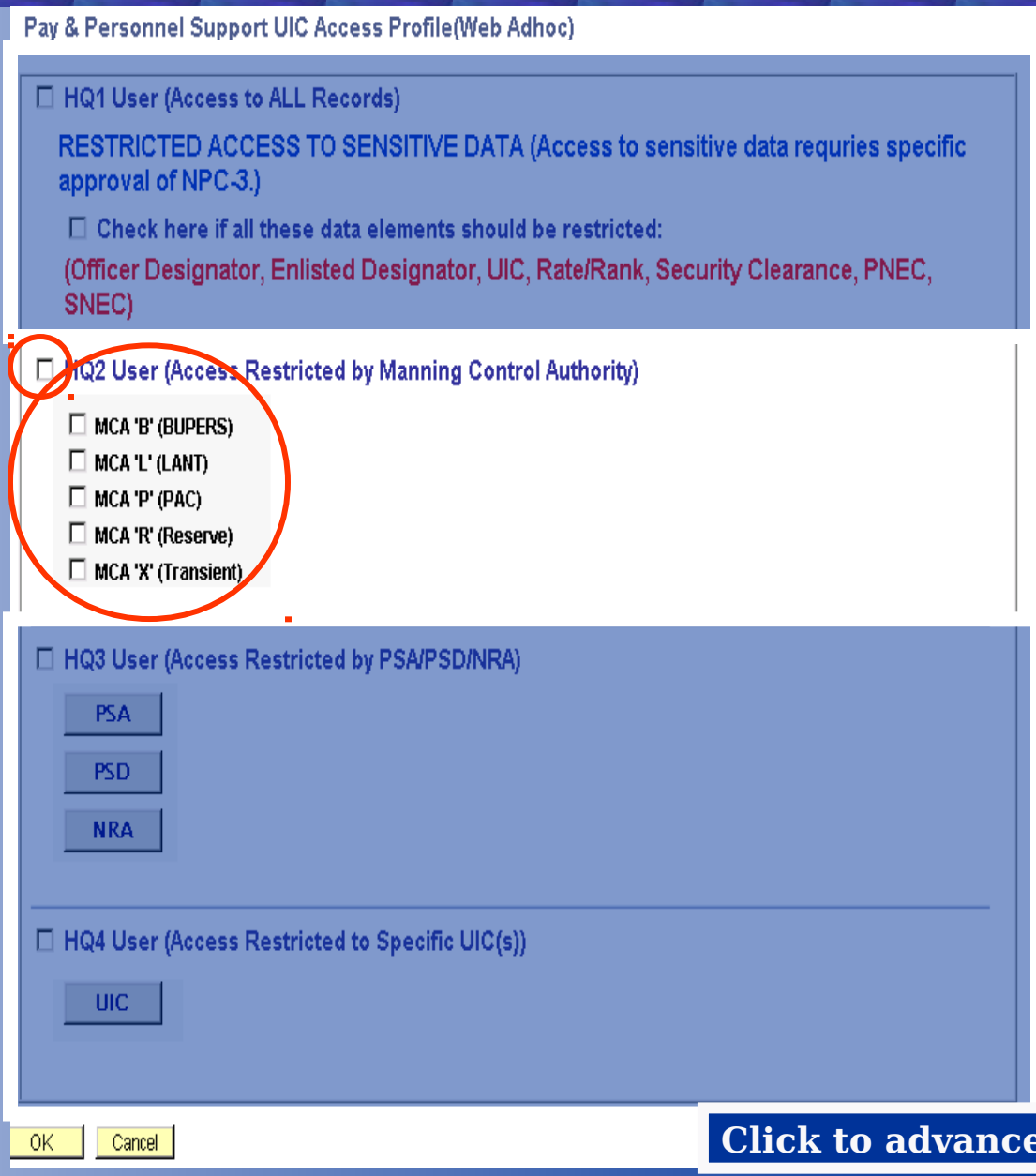

Pay & Personnel Support UIC Access Profile(Web Adhoc)
HQ1 User (Access to ALL Records)
RESTRICTED ACCESS TO SENSITIVE DATA (Access to sensitive data requries specific approval of NPC-3.)
Check here if all these data elements should be restricted:
(Officer Designator, Enlisted Designator, UIC, Rate/Rank, Security Clearance, PNEC, SNEC)
HQ2 User (Access Restricted by Manning Control Authority)
MCA 'B' (BUPERS)
MCA 'L' (LANT)
MCA 'P' (PAC)
MCA 'R' (Reserve)
MCA 'X' (Transient)
HQ3 User (Access Restricted by PSA/PSD/NRA)
PSA
PSD
NRA
HQ4 User (Access Restricted to Specific UIC(s))
UIC
OK
Cancel
Click to advance

SAAR - Web Adhoc

- **HQ2- Manning Control Authority**
  - **MCA ‘B’ - BUPERS**
  - **MCA ‘L’ - LANT**
  - **MCA ‘P’ - PAC**
  - **MCA ‘R’ - Reserve**
  - **MCA ‘X’ - Transient**

HQ2 Should be checked if the User will need access to one of the Manning Control Authorities.

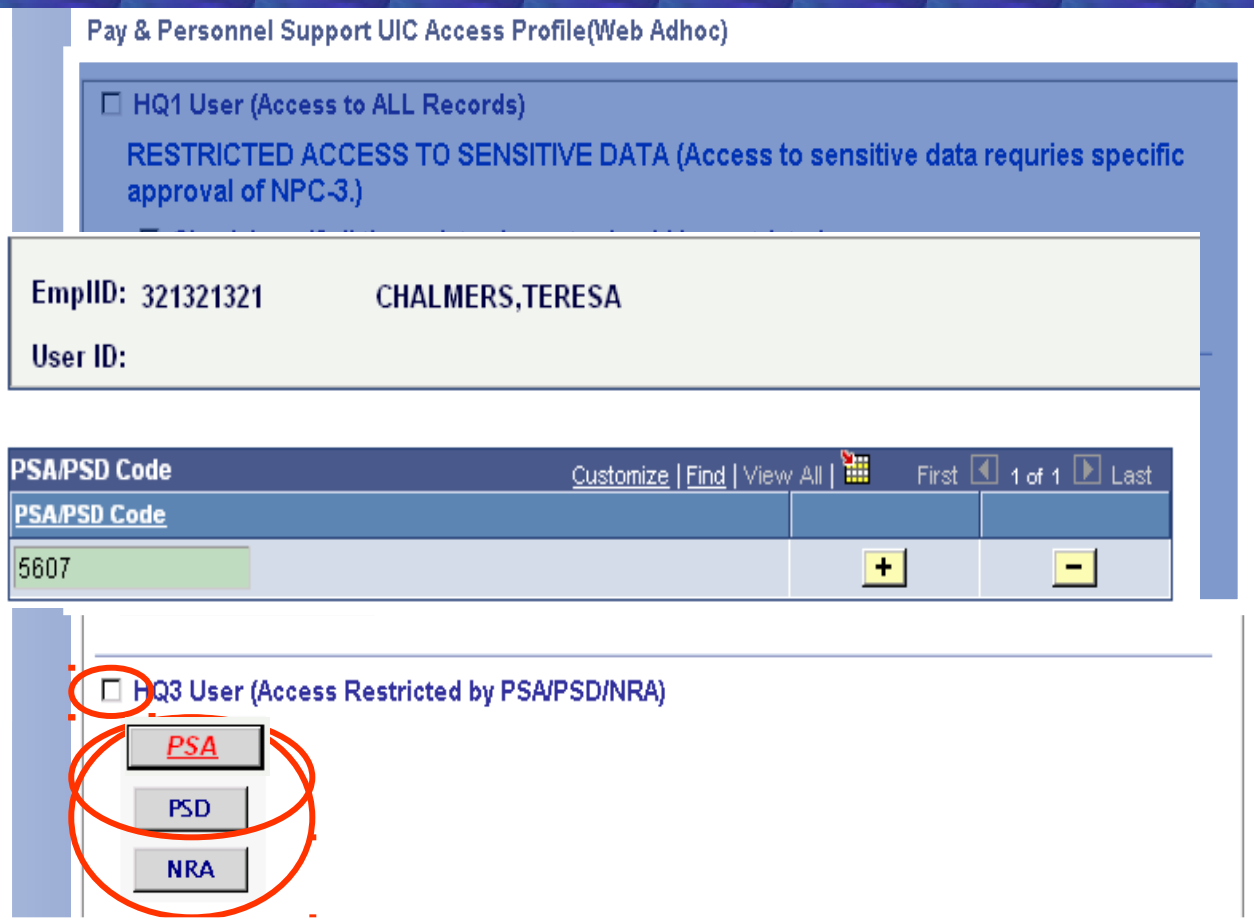
Check the box for the appropriate MCA.


Pay & Personnel Support UIC Access Profile(Web Adhoc)
HQ1 User (Access to ALL Records)
RESTRICTED ACCESS TO SENSITIVE DATA (Access to sensitive data requries specific approval of NPC-3.)
Check here if all these data elements should be restricted:
(Officer Designator, Enlisted Designator, UIC, Rate/Rank, Security Clearance, PNEC, SNEC)
HQ2 User (Access Restricted by Manning Control Authority)
MCA 'B' (BUPERS)
MCA 'L' (LANT)
MCA 'P' (PAC)
MCA 'R' (Reserve)
MCA 'X' (Transient)
HQ3 User (Access Restricted by PSA/PSD/NRA)
PSA
PSD
NRA
HQ4 User (Access Restricted to Specific UIC(s))
UIC
OK
Cancel
Click to advance

SAAR -Web Adhoc

The HQ3 button

- HQ3-PSA/PSD/NRA
  - Add Codes (ADSN) or UIC's under the appropriate button for access
  - Add multiple UICs by using the plus sign
  - The Button will italicize once Code or UIC has been entered


Pay & Personnel Support UIC Access Profile(Web Adhoc)
HQ1 User (Access to ALL Records)
RESTRICTED ACCESS TO SENSITIVE DATA (Access to sensitive data requries specific approval of NPC-3.)
EmplID: 321321321 CHALMERS,TERESA
User ID:
PSA/PSD Code
Customize | Find | View All | First 1 of 1 Last
PSA/PSD Code
5607
HQ3 User (Access Restricted by PSA/PSD/NRA)
PSA
PSD
NRA

The user will enter either the PSA/PSD code under the PSA button or PPS UIC under the PSD button.

If the PSA/PSD code is entered under the PSA button the PPS UIC does not have to be entered under the PSD button.

For Reserve NRA's, enter the UIC under the NRA button.

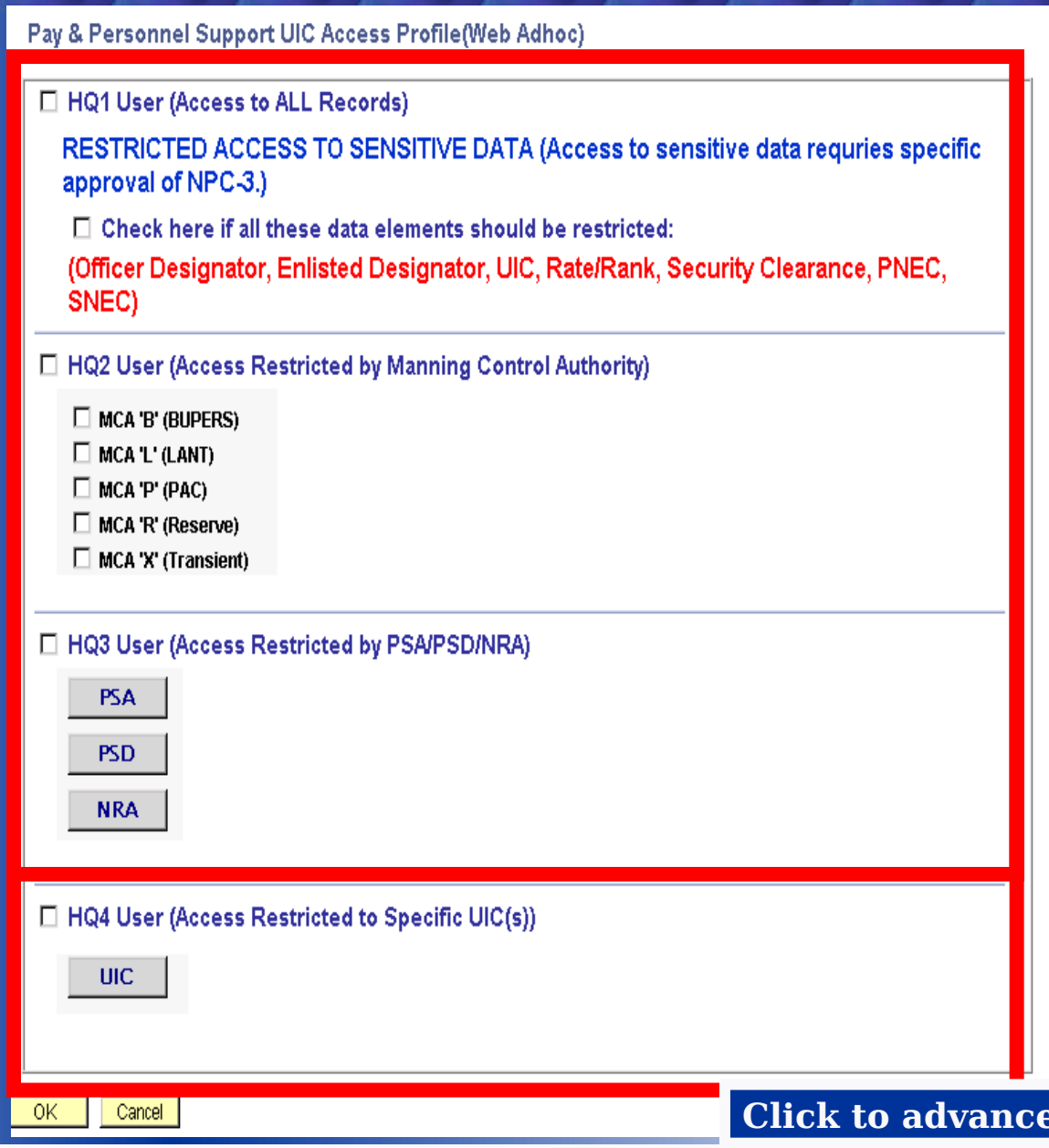
Access will be granted to all UICs under that code or UIC.

Click to advance

SAAR -Web Adhoc

- HQ1, HQ2 and HQ3 access can not be approved locally. All request for these accounts MUST be approved by the SUPER NAM at PERS-3

- HQ4 will be approved by the Local NAM


Pay & Personnel Support UIC Access Profile(Web Adhoc)
HQ1 User (Access to ALL Records)
RESTRICTED ACCESS TO SENSITIVE DATA (Access to sensitive data requries specific approval of NPC-3.)
Check here if all these data elements should be restricted:
(Officer Designator, Enlisted Designator, UIC, Rate/Rank, Security Clearance, PNEC, SNEC)
HQ2 User (Access Restricted by Manning Control Authority)
MCA 'B' (BUPERS)
MCA 'L' (LANT)
MCA 'P' (PAC)
MCA 'R' (Reserve)
MCA 'X' (Transient)
HQ3 User (Access Restricted by PSA/PSD/NRA)
PSA
PSD
NRA
HQ4 User (Access Restricted to Specific UIC(s))
UIC
OK
Cancel

Click to advance

Next Segment is Forgotten Passwords

Forgotten Passwords

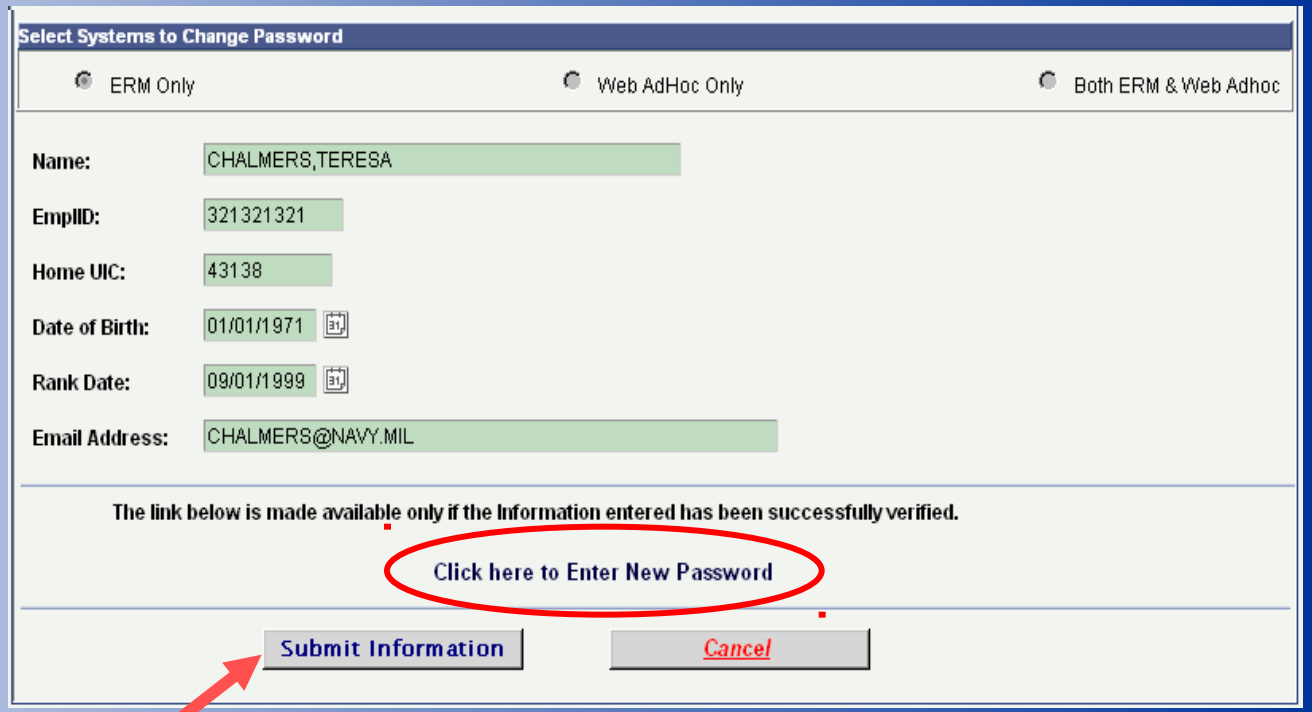
The Users of ERM/NSIPS, Web AdHoc and Self Serve passwords can be reset from the log on screen

- Enter the Operator Id
- Must match exactly as the original SAAR form and is case sensitive
- Tab out of field
- An input panel will appear for the user to validate information

Click to advance

Forgotten Passwords

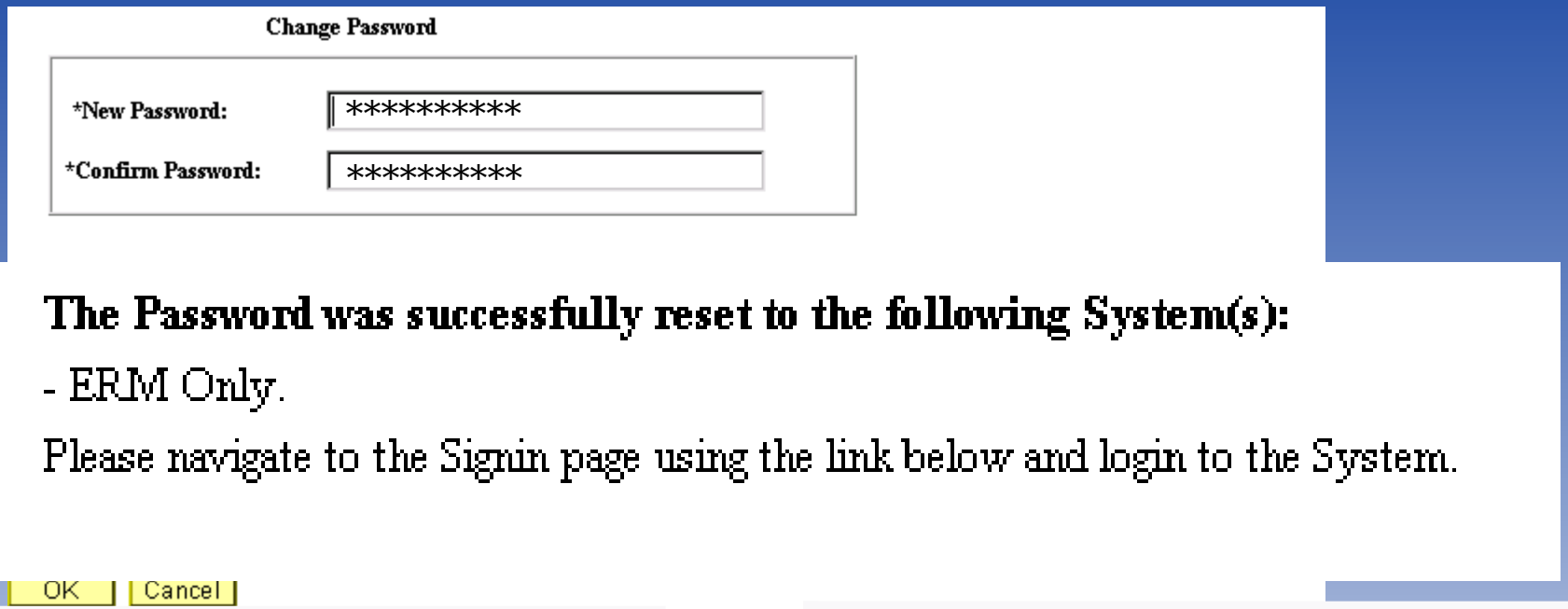
- Questions will be asked for verification
- User will fill in the text fields
- All information must match the original SAAR form or database
- Click the Submit Information button for verification



- Once information is verified the link will highlight
- Select this link to open the change Password panel

Click to advance

Forgotten Passwords



- The users will enter the new password and confirm
- The user has the option of changing passwords in the NSIPS/ERM,to include Self Serve, WEB Adhoc or both systems
- Confirming message will appear at which point the user is now able to log into the system
- Passwords can not be re-used. The database maintains an infinite password log

Click to advance

Next Segment is NAM Functions, Worklist and Reports

If you **will not** be a NAM, but **will** maintain a Self Serve account (Active, Reserve Navy members) Click here to advance to Self Serve segment

If you **will not** be a NAM, or **will not** maintain a Self Serve account click here to end the show

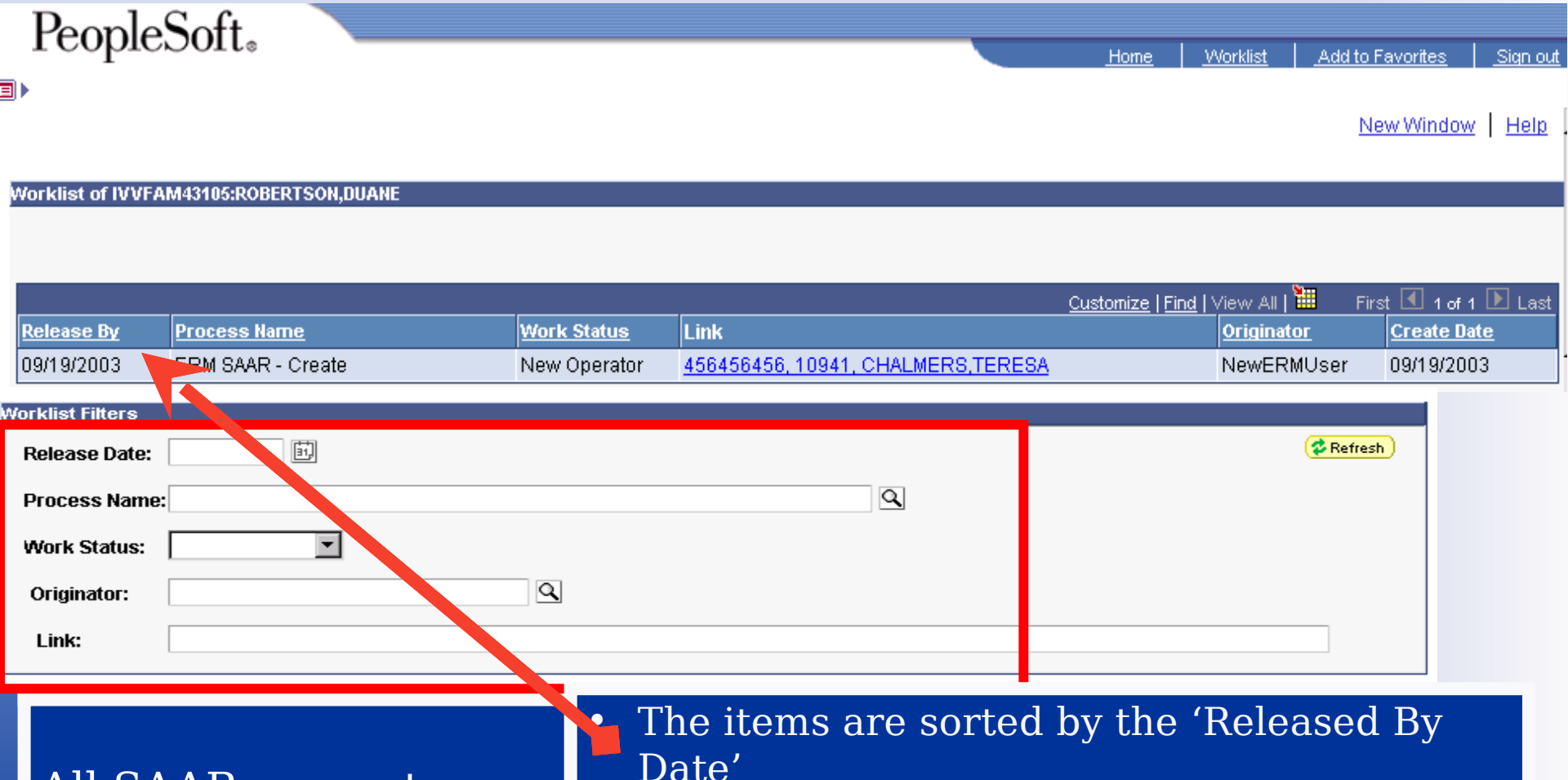
Click to continue to the NAM Functions segment

NAM Function -Worklist

SAAR forms submitted will be found in the worklist of the individual ISSO/FAM that the user chose.

Click to advance

NAM Function - Worklist

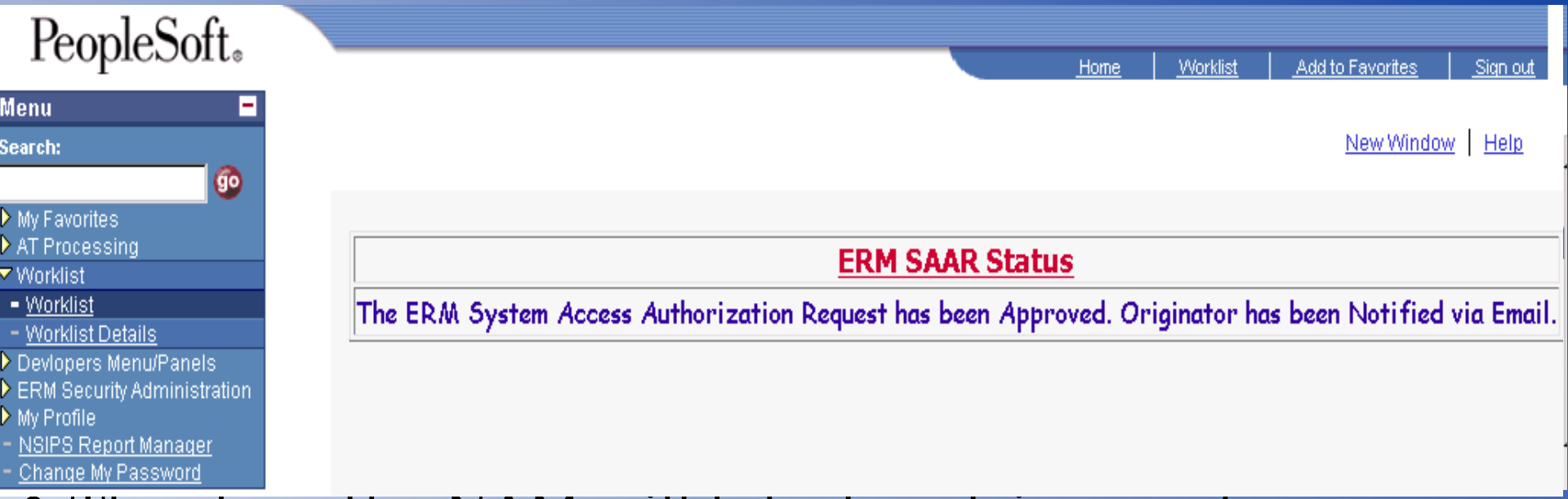

PeopleSoft
Home | Worklist | Add to Favorites | Sign out
New Window | Help
Worklist of IVVFAM43105:ROBERTSON,DUANE
Customize | Find | View All | First 1 of 1 Last
Release By | Process Name | Work Status | Link | Originator | Create Date
09/19/2003 | ERM SAAR - Create | New Operator | 456456456, 10941, CHALMERS,TERESA | NewERMUser | 09/19/2003
Worklist Filters
Refresh
Release Date:
Process Name:
Work Status:
Originator:
Link:

All SAAR request awaiting NAM approval will be located in the Worklist

- The items are sorted by the 'Released By Date'
  - search/filter option has been added
  - All items routed, via workflow, will be shown in their worklist, unless the list is narrowed using the filter opti

Click to advance

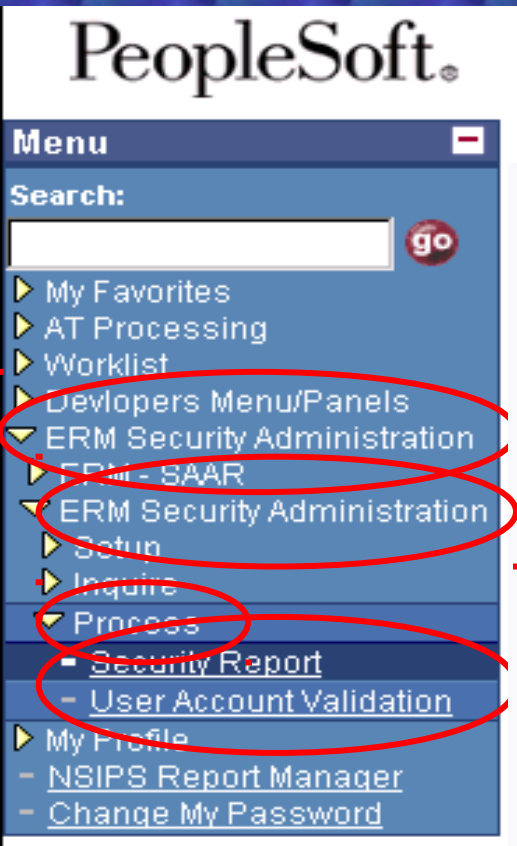
NAM Function - Worklist



- The steps the NAM will take to retrieve and approve a SAAR request
  - Access the worklist
  - Select the item to be worked
  - Review the request for accuracy
  - Make appropriate changes if needed
  - Select the approve or deny button at the bottom of the SAAR request

Click to advance

NAM Functions - Reports



- The navigation string is as follow
  - ERM Security Administration
  - ERM Security Administration
  - Process
  - User Security Report and Account Validation

- Two Reports the NAM will run
  - Security Report
  - User Account Validation

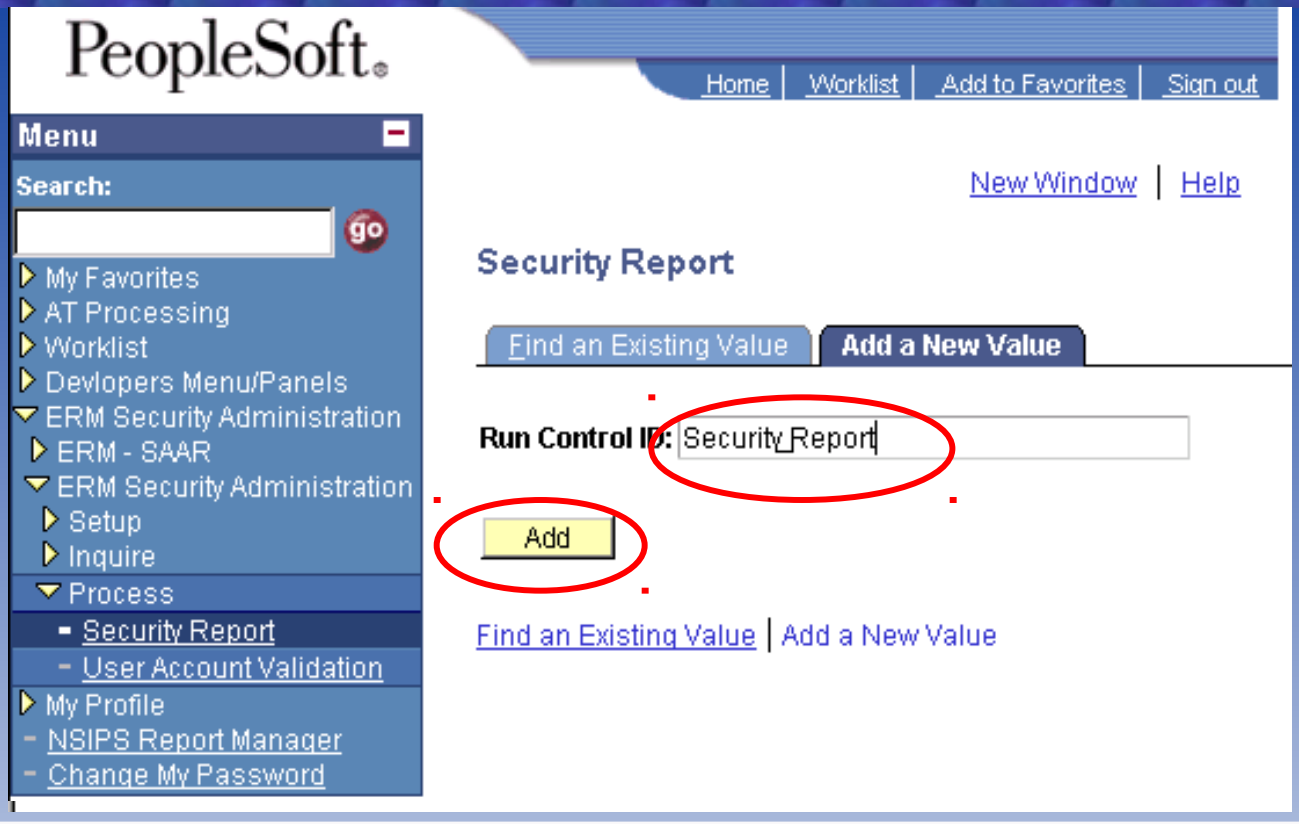
Click to advance

NAM Functions - Reports

- From the “Find an Existing Value” panel enter the Run Control Id of an existing report or use the Search button to choose from all existing reports

Click to advance

NAM Functions - Reports



- If a new Report is to be Generated
  - Click on the “Add a New Value” link.
  - A new panel will appear,
  - Enter the Run Control ID name
  - Select the ADD button to open the Report Criteria panel

Click to advance

NAM Functions - Reports

- The Security Report can be ran as a consolidated Report or narrowed to a specific subject
  - Detail
  - Modified
  - Created
  - Locked
  - Awaiting Approval
  - Inactive

Once the criteria is selected click the Run button this will open the Process Scheduler

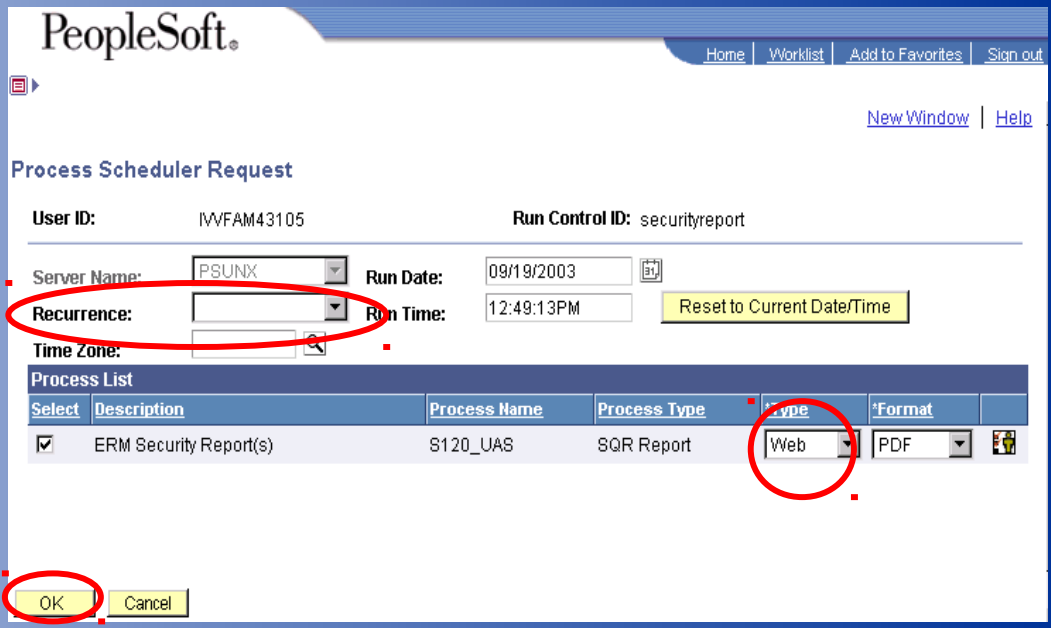
To create a report the user will need to check the box next to the information to be generated.

Click to advance

Process Scheduler

- To set the report for reoccurrence choose a time option under the Recurrence drop down, Leave blank if recurrence is not needed

- **Select how the Report should be generated**
  - **Web**
  - **File**
  - **Email**
  - **Printer**



- **Select the OK button when the Report is ready to be Scheduled This will return the user back to the Criteria panel**

- **The Criteria panel will return with the Process Instance number located under the Run Button**

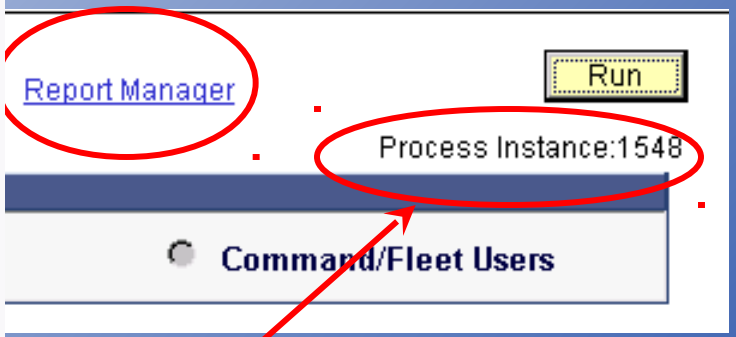
Click to advance

Report Manager

Click the Report Manager Link to open the Report manger panel

Ensure the Process Instance number matches the Report generated

When 'Posted' appears under Status, a view button appears. The user can click the button to retrieve the report



PeopleSoft

Home | Worklist | Add to Favorites | Sign out

New Window | Help

Report List | Server List

Reports Filter

*View Reports: Admin Process Type: SQR Report Refresh

Status: Last: 1 Days

Report List Customize | Find | View All | First 1-2 of 2 Last

Process Name	User ID	Process Instance	Report Description	Request Date/Time	Format	Status	Details	View Report
S120_UAS	IWFAM43105	1548	ERM Security Report(s)	09/19/2003 12:49:55PM	Acrobat (*.pdf)	Posted	Details	View
S117_UAV	IWFAM43105	1519	User Account Validation	09/18/2003 2:05:32PM	Acrobat (*.pdf)	Posted	Details	

Click to advance

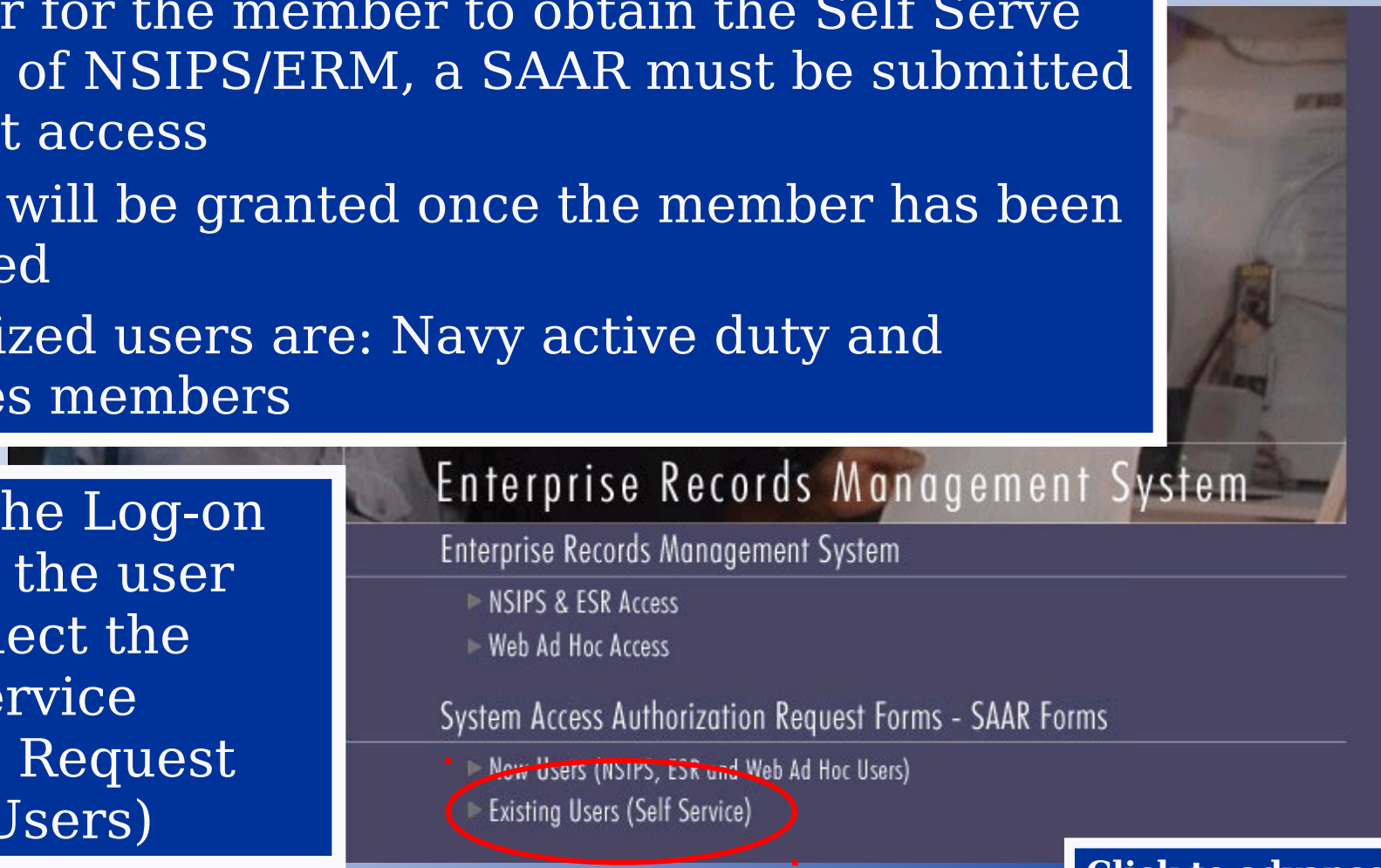
Next Segment is Self Serve SAAR Submission

Click to advance

Self Serve - SAAR form

- In order for the member to obtain the Self Serve portion of NSIPS/ERM, a SAAR must be submitted to grant access
- Access will be granted once the member has been validated
- Authorized users are: Navy active duty and reserves members

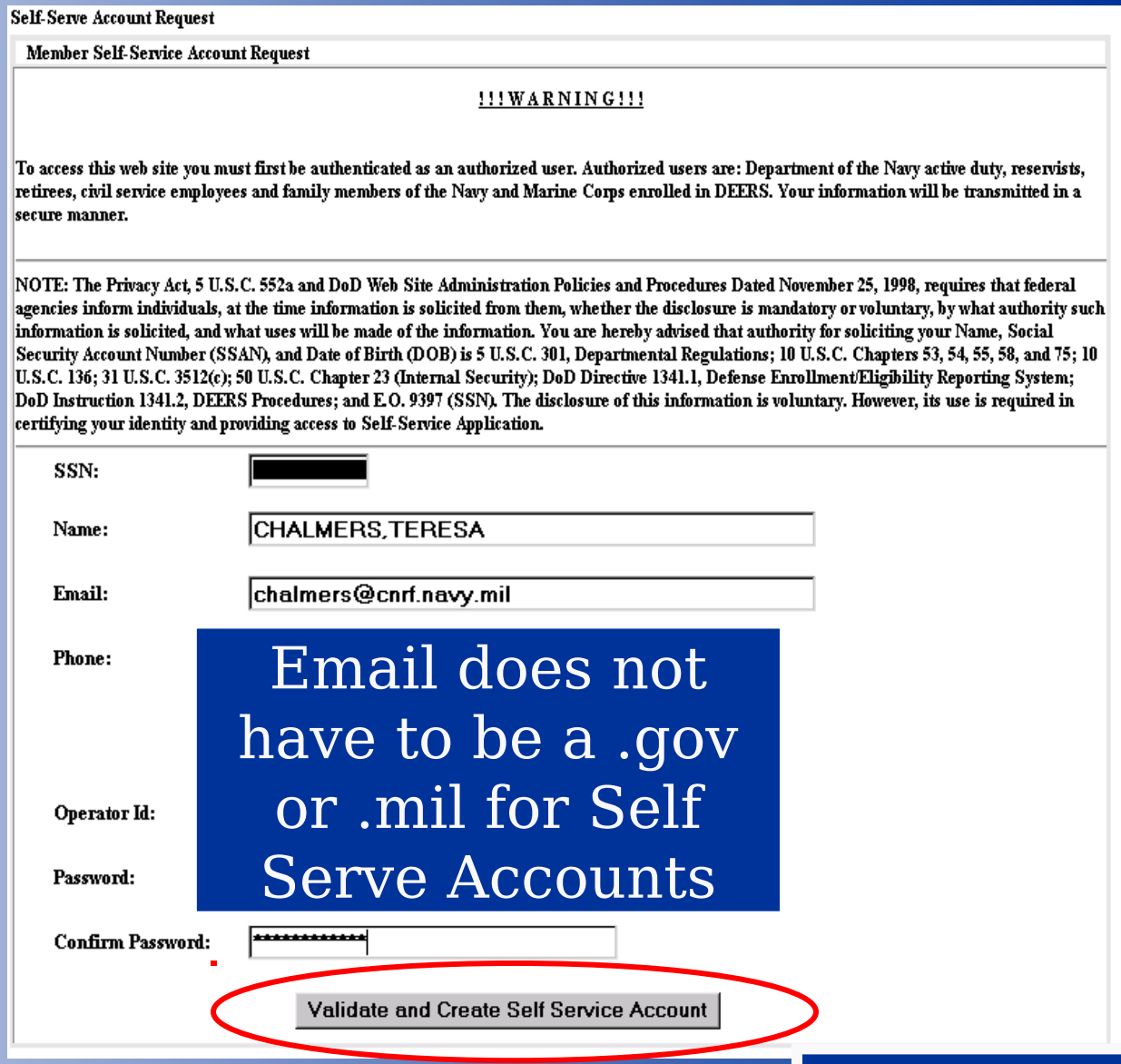
- From the Log-on screen the user will select the Self-Service UserId Request (New Users)


Enterprise Records Management System
Enterprise Records Management System
NSIPS & ESR Access
Web Ad Hoc Access
System Access Authorization Request Forms - SAAR Forms
Existing Users (Self Service)

Click to advance

Self Serve - SAAR form

- The member must fill out the information and choose an Operator Id and password
- The Same criteria for OperIds and Passwords are the same as the User SAAR
- Click the Validate button to create the Self Serve Account


Self-Serve Account Request
Member Self-Service Account Request
!!!WARNING!!!
To access this web site you must first be authenticated as an authorized user. Authorized users are: Department of the Navy active duty, reservists, retirees, civil service employees and family members of the Navy and Marine Corps enrolled in DEERS. Your information will be transmitted in a secure manner.
NOTE: The Privacy Act, 5 U.S.C. 552a and DoD Web Site Administration Policies and Procedures Dated November 25, 1998, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Name, Social Security Account Number (SSAN), and Date of Birth (DOB) is 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. Chapters 53, 54, 55, 58, and 75; 10 U.S.C. 136; 31 U.S.C. 3512(c); 50 U.S.C. Chapter 23 (Internal Security); DoD Directive 1341.1, Defense Enrollment/Eligibility Reporting System; DoD Instruction 1341.2, DEERS Procedures; and E.O. 9397 (SSN). The disclosure of this information is voluntary. However, its use is required in certifying your identity and providing access to Self-Service Application.
SSN:
Name:
CHALMERS,TERESA
Email:
chalmers@cnrf.navy.mil
Phone:
Operator Id:
Password:
Confirm Password:
Validate and Create Self Service Account
Email does not have to be a .gov or .mil for Self Serve Accounts

Click to advance

Self Serve - SAAR form

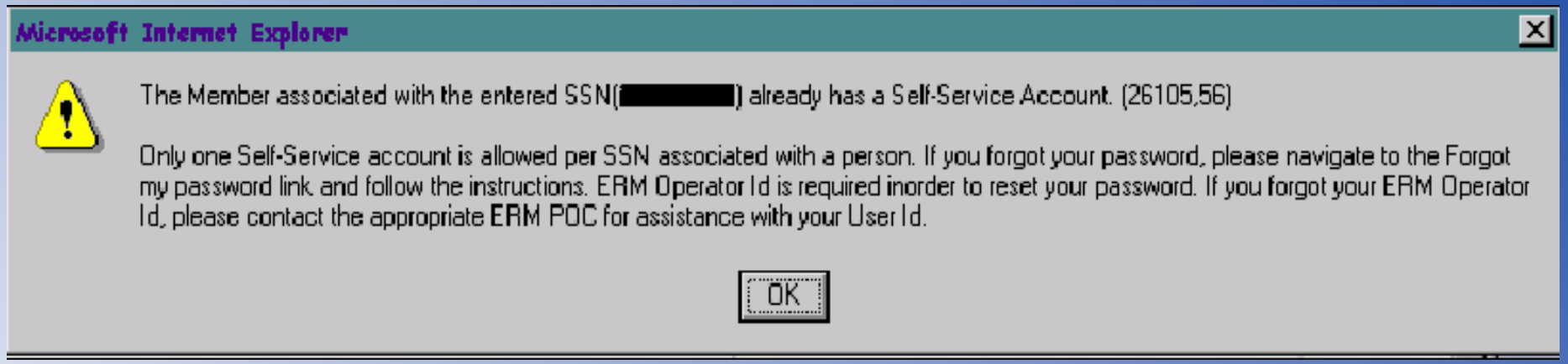
Microsoft Internet Explorer
Entered SSN :123123123 does not have a record at ERM database. (26107,1)
Cannot request Self-Service User Account for this SSN.
OK

- **If the member's SSN is not in ERMS the request will be denied**
- **If the SSN input is valid and receives this error, the member must contact the NSIPS helpdesk**

Click to advance

Self Serve - SAAR form

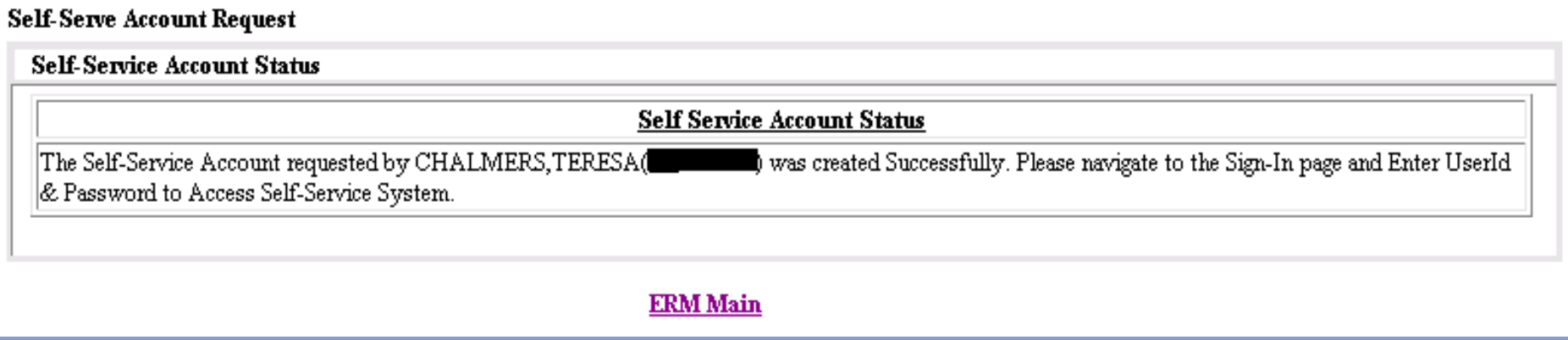
- If a member is attempting to set up a self serve account and receives the displayed error. This indicates that the requested SSN has a Self Serve account activated.


Microsoft Internet Explorer
The Member associated with the entered SSN([redacted]) already has a Self-Service Account. (26105,56)
Only one Self-Service account is allowed per SSN associated with a person. If you forgot your password, please navigate to the Forgot my password link and follow the instructions. ERM Operator Id is required inorder to reset your password. If you forgot your ERM Operator Id, please contact the appropriate ERM POC for assistance with your User Id.
OK

- The Helpdesk must be notified if the member gets this error and the member had not previously activated the account. This means that an unauthorized user has accessed this account and this is now a security issue.

Click to advance

Self Serve - SAAR form


Self-Serve Account Request
Self-Service Account Status
Self Service Account Status
The Self-Service Account requested by CHALMERS,TERESA([redacted]) was created Successfully. Please navigate to the Sign-In page and Enter UserId & Password to Access Self-Service System.
ERM Main

- Once the sign up page is complete and the validate button is selected the user will get a message stating that the account is now created and at this point the user is now able to review the account.

Click to advance

This concludes the SAAR presentation

Click to End Sho